
# WINDOWS-PALVELIMIEN TIETOTURVATASON RAPORTOINTI

**Opinnäytetyö**

**Mikko Goman**

**Tietotekniikan koulutusohjelma**
Tietoverkot

**SAVONIA-AMMATTIKORKEAKOULU TEKNIIKKA KUOPIO**

Koulutusohjelma

Tietotekniikan koulutusohjelma, tietoverkot

Tekijä

Mikko Goman

Työn nimi

Windows-palvelimien tietoturvan raportointi

| Työn laji | Päiväys | Sivumäärä |
|---|---|---|
| Opinnäytetyö | 15.4.2010 | 48 |

| Työn valvoja | Yrityksen yhdyshenkilö |
|---|---|
| FL. filosofian lisensiaatti Veijo Honkonen | Järjestelmäinsinööri Marko Ruotsala |

Yritys

Kuopion yliopistollinen sairaala, Tekplus

Tiivistelmä


Opinnäytetyö tehtiin Pohjois-Savon sairaanhoitopiirin tekniselle tukiyksikölle, Tekplus:lle. Opinnäytetyön aiheena oli kartoittaa Windows-palvelimien tietoturvataso ja luoda saaduista tuloksista tietoturvaraportit. Työn tavoitteena oli kehittää mielekkäät raportointityökalut ja menetelmät tulevia tietoturvakartoituksia varten. Tietoturvakartoituksien lisäksi opinnäytetyöhön kuului käyttäjäryhmien oikeuksien kartoitus.

Opinnäytetyön pääpaino oli palvelimien tietoturvatason kartoituksessa ja käyttäjäryhmien oikeuksien määrittämisessä. Työhön käytettiin Nessus 4.0.2 -tietoturvaskanneria ja PC Remote Permissions Audit -ohjelmaa.Tietoturvaraportointia varten laadittiin raportointipohjat ja kartoituksiin käytetyistä ohjelmista tehtiin pikaoppaat. Tietoturvakartoituksia varten mietittyjä menetelmiä sovellettiin opinnäytetyön aikana muutamaan testipalvelimeen ja yhteen tuotantokäytössä olleeseen ISA-julkaisupalvelimeen.

Palvelimia tarkasteltiin järjestelmällisesti kummallakin ohjelmalla ja saaduista tuloksista laadittiin Microsoft Word 2003:lla tietoturvaraportit. Ohjelmien löytämät tiedot esiteltiin ja analysoitiin raporteissa. Raportit kirjoitettiin opinnäytetyön aikana laaditulle raporttipohjalle. Kokonaisuutena opinnäytetyön tavoitteet saavutettiin. Työn luonteen vuoksi tässä opinnäytetyössä ei käydä läpi tietoturvakartoituksien tuloksia.



Avainsanat

tietoturva, windows-palvelimet, nessus

Luottamuksellisuus

julkinen

**SAVONIA UNIVERSITY OF APPLIED SCIENCES**

Degree Programme

Information Technology

Author

Mikko Goman

Title of Project

Reporting Information Security of Windows Servers

| Type of Project | Date | Pages |
|---|---|---|
| Final Project | 15. April 2010 | 48 |

| Academic Supervisor | Company Supervisor |
|---|---|
| Mr. Veijo Honkonen | Mr. Marko Ruotsala |

Company

Kuopio University Hospital, Tekplus

Abstract

This final project was made for Technical Support Unit of Northern Savo Healthcare District. The main goal of this project was to scan the data security level of the Windows servers used in the healthcare district and report the results. In addition to data security scans, one of the main goals of this final project was to map the rights of certain user groups in the domains used in the healthcare district. Another goal was to devise suitable methods for upcoming scans.

The Nessus 4.0.2 security scanner was used to scan security levels and the PC Remote Permissions Audit program was used to map user rights for certain groups. Each of the servers were systematically scanned with both programs. The results were reported using Microsoft Word 2003. The reports were made on a separate report template, which was made during this project. In addition, a set of instructions were drawn up. During the final project, these methods were tested on several test servers and one in-service ISA publishing server.

The results were analyzed and displayed in the reports. As a whole, the goals of this project were achieved. None of the results obtained from the scans are shown in this document due to the nature of this project.

Keywords

data security, Nessus

Confidentiality

public

## Alkusanat

Olin työharjoittelussa Kuopion yliopistollisen sairaalan teknisessä tukiyksikössä Tekplus:ssa 8.7.2009 - 31.12.2009. Olin ensin töissä tietotekniikkayksikön lähituessa, minkä jälkeen siirryin palvelinyksikön puolelle. Tämä opinnäytetyö tehtiin palvelinyksikölle. Ennen opinnäytetyön aloittamista tein lähituen piiriin kuuluvia töitä, joihin kuuluivat mm. koneiden korjaus ja asennus, oheislaitteiden asennus ja ohjelmistojen asennuksia. Lähituessa vietettyjen viikkojen aikana opin sairaalan tietotekniikasta paljon, mikä auttoi huomattavasti siirtyessäni palvelinyksikön puolelle. Palvelinyksikössä suorittamani ylläpitotehtävät ja lähituen tukitoimet lisäsivät kuuden kuukauden aikana tietoteknistä osaamistani valtavasti.

Haluan kiittää järjestelmäinsinööri Jouni Suhosta ja järjestelmäinsinööri Marko Ruotsalaa mahdollisuudesta työskennellä Tekplus:ssa ja mahdollisuudesta tehdä opinnäytetyö palvelinyksikölle. Kiitän myös filosofian lisensiaatti Veijo Honkosta mainiosta opinnäytetyönohjauksesta. Lisäksi haluan kiittää tietotekniikkayksikön jäseniä tuesta ja avusta koko työssäoloni ajalta. Heidän avullaan ammattitaitoa kertyi paljon ja opin asioita, joita koulussa ei opeteta.

Kuopiossa 15.4.2010

_____

Mikko Goman

# Sisällys

# 1 JOHDANTO

Tämä opinnäytetyö tehtiin Kuopion Yliopistollisen sairaalan teknisen tukiyksikön, Tekplus:an pyynnöstä marras- ja joulukuun 2009 välisenä aikana. Tekplus oli Kuopion Yliopistollisen Sairaalan ja Pohjois-Savon sairaanhoitopiirin (PSSHP) alueella toimiva tekninen yksikkö, johon kuului useita eri teknisen alan osaamisyksiköitä, esimerkiksi tietotekniikkatuki, sovellustuki ja lääkelaitehuolto. Yhteensä Tekplus työllisti vakituisesti noin 60 henkilöä. Tekplus:an tulosjohtajana toimi yksikön vielä toimiessa Pasi Markkanen. Tämä opinnäytetyö tehtiin Tekplus:an tietotekniikkayksikölle. Opinnäytetyöni ohjaajana KYS:n puolelta toimi järjestelmäinsinööri Marko Ruotsala, joka oli myös tämän opinnäytetyön aikana aloitetun projektin vetäjä loppuvuoden 2009.

Tekplus yhdistyi 1.1.2010 Kuopion kaupungin atk-keskuksen kanssa muodostaen Istekki Oy:n ja tämä projekti siirtyi yhdistymisen mukana Istekki Oy:lle. Tämän osakeyrityksen toimitusjohtajaksi valittiin Urpo Karjalainen. Syntyneen yrityksen omistavat yhdessä Kuopion kaupunki ja Pohjois-Savon sairaanhoitopiiri. Yritys tarjoaa PSSHP:lle ja Kuopion kaupungille samoja palveluja, joita Tekplus ja kaupungin atk-keskus aikanaan tarjosivat. Tekplus:an yhdistyminen Kuopion kaupungin atk-keskuksen kanssa tulee kuitenkin todennäköisesti viivyttämään projektin jatkamista, mutta olemassa olevat työkalut siihen mahdollistaisivat sen, ettei aloitukseen enää tarvitse käyttää resursseja.

Syy projektin aloittamiselle oli tarve selvittää PSSHP:n käyttämien palvelimien tietoturvataso ja karsia riskiryhmien oikeuksia palvelimille. Näillä toimilla parannettaisiin sairaanhoitopiirin tietojärjestelmien tietoturvaa ja pienennettäisiin mahdollisia tietoturvariskejä. Projekti käynnistyi marraskuun alussa 2009. Opinnäytetyö rajattiin kattamaan vain projektin alkuvaiheet. Palvelimien suuren määrän vuoksi, tässä dokumentissa käsitellään vain projektin aloitus, testausmenetelmien kehitys projektin jatkoa varten ja tietoturvaraporttipohjan laatiminen. Opinnäytetyön aikana kerätyt tiedot palvelimista eivät ole julkista tietoa, joten niitä ei esitellä tässä dokumentissa.

Opinnäytetyön tavoite oli luoda järkevät kartoitusmenetelmät ja etsiä työkalut sekä testata niitä testipalvelimiin. Näin tehtiin pohjatyö toimialueen tuotantopalvelimien kartoi-

tuksille. Projektin tavoite oli saada kokonaisuudessaan kartoitettua kaikkien KYS:n ja PSSHP:n käyttämien palvelimien tietoturva. Opinnäytetyön aikana kartoituksia tehtiin vain muutamalle palvelimelle. Opinnäytetyön aikana tehdyt tietoturvakartoitukset tehtiin suunnitelmien mukaan Tenablen valmistamalla Nessus 4.0.2 -tietoturvaohjelmalla. Opinnäytetyön aikana kartoitettiin riskiryhmien oikeudet tiedostojakoihin, paikallisiin tiedostoihin ja kansioihin. Käyttäjäryhmien kartoitukseen käytettävä ohjelma valittiin projektin aikana.

Opinnäytetyön aikana mietittyjä kartoitusmenetelmiä ja ohjelmia sovellettiin testipalvelimiin, joista ensimmäiset raportit kirjoitettiin. Testipalvelimien lisäksi näitä menetelmiä testattiin tuotantokäytössä olevaan ISA-julkaisupalvelimeen (Microsoft Internet Security & Acceleration Server), jotta menetelmien luotettavuus ja tehokkuus voitiin todeta tuotantoympäristössä. Opinnäytetyön aikana kirjoitettiin pienimuotoinen asennus- ja käyttöopas ohjelmista. Tietoturvaraportin pohjan tarkoitus oli helpottaa uusien raporttien tekoa niistä palvelimista, joita tämän työn aikana ei kartoitettu. Valmiiksi etsitty ohjelma käyttäjäryhmien oikeuksien kartoitukseen auttaa projektin jatkamista tämän opinnäytetyön ulkopuolella

# 2 WINDOWS PALVELIMET

## 2.1 Yleistä

Windowsin käyttöjärjestelmiä on olemassa työasemakäyttöön ja palvelinkäyttöön. Tässä luvussa käydään läpi lyhyesti, mitä palvelinratkaisuja Windows-palvelimissa on olemassa. Windows-palvelimen käyttöjärjestelmä eroaa normaalista työasemakäyttöjärjestelmästä siten, että palvelin pystyy tarjoamaan toimialueelle erilaisia palveluita. Näitä palveluita ovat esim. toimialueen ohjauskoneena toimiminen (Domain Controller), tiedostopalvelin, tietokantapalvelin ja DHCP-palvelin.

Opinnäytetyön aikana tehdyt tietoturvakartoitukset tehtiin Windows Server 2003 ja 2008 -palvelimiin sekä yhteen ISA-julkaisupalvelimeen.

## 2.2 Windows-käyttöjärjestelmät palvelimissa

Palvelinkäytössä on tällä hetkellä kolme eri Windows-palvelin sukupolvea. Nämä ovat Windows 2000 Server, Windows Server 2003 ja Windows Server 2008. Näistä vanhin, Windows 2000 Server on väistymässä käytöstä. Sen tuotetuki päättyy 13. heinäkuuta 2010.

Windows Server 2003 julkaistiin huhtikuussa 2003 korvaamaan Windows 2000 Server. Siitä julkaistiin kolme eri versiota: Windows 2003 Standard Edition (peruspalvelimeksi, esim. tiedostopalvelin), Windows 2003 Enterprise Edition (raskaaseen palvelinkäyttöön, tarjoaa klusterointimahdollisuudet) ja Windows 2003 Datacenter edition (saatavilla 32- ja 64-bittisenä). Lisäksi Windows Server 2003:sta julkaistiin erillinen, pelkästään web-julkaisuihin tarkoitettu Windows Server 2003, Web Edition. Windows Server 2003 vastasi käyttöliittymältään Windows XP:tä pienin eroavaisuuksin. Uusina ominaisuuksina se toi mukanaan tuen .NET-sovelluksille sekä paremman laajennettavuuden ja skaalauksen klustereiden ja symmetrisen moniprosessoinin avulla (Symmetric MultiProcessing). Tietoturva oli yksi tärkeimpiä osa-alueita Windows Server 2003:sen kehityksessä. Merkittävin uutuus näistä oli IIS (Internet Information Services) 6.0:n julkaisu. Windows 2000 Server:in julkaisun yhteydessä esiteltyjä ominaisuuksia paranneltiin Windows

Server 2003:ssa. Uuden Windows Server 2008 R2:sen ilmestyminen merkitsee sitä, että Windows Server 2003:n ns. mainstream tuotetuki loppuu 13. heinäkuuta 2010, jonka jälkeen se siirtyy jatketun tuen vaiheeseen, joka kestää aina vuoteen 2015 asti. Tämä tarkoittaa sitä, että siirtymävaihe 2003:sta uuteen 2008 R2:een on jo alkanut. [1][2, s.13-14]

Windows Server 2008 julkaistiin 27. helmikuuta 2008 ja sen paranneltu versio Windows Server 2008 R2 heinäkuun 22. 2009. Tästä uudesta R2:sta julkaistiin useita eri versioita. Windows Server 2008 R2 Foundation, Standard, Enterprise, Datacenter, Web Server ja HPC Server. Kuten Windows Server 2003 -julkaisut, myös Windows Server 2008:n versiot eroavat toisistaan ominaisuuksiltaan siten, että perusversiot sopivat kevyempään käyttöön ja suuremmat raskaaseen palvelinkäyttöön. Uusina ominaisuuksina Windows Server 2008 R2 toi paremman laitetuen siirtyen samalla pelkästään 64-bittiseen ympäristöön, uusia virransäästö ominaisuuksia, virtuaalitekniikat Hyper-V:n ja VDI:n (Virtual Desktop Interface), parannuksia palvelimien hallintaan ja uuden IIS 7.5 -version. Windows Server 2008 R2 on suunniteltu korvaamaan Windows Server 2003. Se perustuu samaan tekniikkaan kuin Windows Vista ja Windows 7. [3]

## 2.3 Microsoft Internet Security & Acceleration Server

Microsoft Internet Security & Acceleration Server eli ISA-palvelin on ohjelmistokerroksella toimiva tilallinen palomuuri, jonka avulla suojataan esim. web-julkaisuja Internetistä tulevia uhkia vastaan. ISA-palvelin tarjoaa siis turvallisen julkaisukanavan yrityksen web-sivuille ja esim. Windows SharePointille. Lisäksi ISA-palvelin pystyy toimimaan VPN-yhteyden päätepisteenä, jolloin yrityksen etätyöntekijät voivat ottaa yhteyden siihen suojattua VPN-tunnelia hyväksi käyttäen.

Uusin versio ISA:sta on Microsoftin uusi Forefront Threat Management Gateway (FTMG) 2010, joka perustuu ISA 2006:n pohjalle. ISA 2006 toimintojen lisäksi FTMG tarjoaa paremman palomuurin, joka ohjelmakerroksen lisäksi tarkastelee verkkokerroksen tapahtumia. Tämä mahdollistaa URL-suodatuksen. Lisäksi ISA pystyy etsimään haittaohjelmia ja toimimaan tunkeutumisestojärjestelmänä. Tunkeutumisestojärjestelmä toimii eräänlaisena IDS-järjestelmänä. Kuten ISA, myös FTMG on suunniteltu suojaa-

maan yrityksen verkkoresursseja ja helpottamaan niiden saatavuutta yrityksen työntekijöille ja asiakkaille. [4][5]

# 3 TIETOTURVA

## 3.1 Yleistä tietoturvasta

Tietoturvalla tarkoitetaan yksilölle tai yhteisölle tärkeän tiedon suojaamista niin, ettei siihen pääse käsiksi asiattomat henkilöt tai tahot. Nykyisessä tietoyhteiskunnassa tietoturvasta on tullut yhä tärkeämpi. Internetin käytön lisääntyminen ja tiedon sähköistyminen ovat lisänneet haasteita tietoturvalle. Opinnäytetyössä käsiteltiin palvelimien tietoturvaa yritys- ja virastoympäristössä, joten tässä luvussa keskitytään palvelimien tietoturvaan ja siihen, millä keinoin yritykset voivat parantaa tietoturvaansa.

Tietoturvalla suojaudutaan ulkoisia ja sisäisiä uhkia vastaan. Nämä uhat voidaan vapaasti luokitella kolmeen ryhmään: tunkeutuminen, palvelunestot ja tietovarkaudet. Ulkoisia uhkia ovat luvattomat yhteydet palvelimeen ja verkkoon esimerkiksi tiettyä tietoturva-aukkoa hyväksi käyttäen. Tietoturva-aukko voi olla auki oleva portti, heikko salaus tai salasana. Luvatonta yhteyttä palvelimeen voidaan käyttää tiedon keräämiseen palvelimista ja verkosta. Tätä tietoa voidaan käyttää hyväksi ja yrittää päästä käsiksi palvelimella oleviin tietoihin. Mikäli tietoliikennettä pystyttäisiin seuraamaan, hyökkääjä voisi teoriassa selvittää käyttäjätunnuksia ja salasanoja. Tietoliikennettä seuraamalla hyökkääjä pystyy keräämään tietoa palvelimien ja verkon suojauksesta. Tiedon keräyksen lisäksi luvattomilla yhteyksillä voidaan häiritä verkon ja palvelimen toimintaa kuormittamalla verkkoa roskaliikenteellä (Denial Of Service, DoS-hyökkäys,). Edellä mainittu hyökkäys on esimerkki palvelunestohyökkäyksestä. Hyökkäyksien takana voi olla yksittäinen henkilö tai ohjelma.

Sisäiset uhkat ovat kuin ulkoiset, mutta niissä hyökkäys tapahtuu verkon sisältä päin. Sisäinen hyökkäys tarkoittaa siis, että hyökkääjä on päässyt fyysisesti kirjautumaan tietoverkkoon ja samalla kiertänyt mahdolliset sisä- ja ulkoverkon väliset palomuurit ja suojaukset. Hyökkääjän on siis helpompi päästä tekemään tuhoja.

Tietoturvan tavoite tietojen suojaamiseksi on hyvin yksinkertainen. Tiedon pitää olla luottamuksellista eli se on saatavilla vain halutuille tahoille ja henkilöille. Tiedon pitää olla eheä. Se ei ole saanut muuttua millään tavalla esim. etäyhteyden aikana. Tietoon ei

voida luottaa, mikäli sen eheys on vaarantunut. Asianomaisten tahojen on saatava tieto helposti ja vaivattomasti. Luotettavuus, eheys ja käytettävyys määrittelevät tietoturvan tavoitteet.[2, s. 29 - 31] [6, s. 28 - 37]

Yritysten kannalta järkevintä on tehdä erillinen tietoturvasuunnitelma ja riskianalyysi, joiden avulla kartoitetaan yrityksen tarpeet ja resurssien kohdennus onnistuisi paremmin. Tietoturvasuunnitelmassa otetaan kantaa mm. palomuureihin, virustorjuntaan, käyttäjien koulutukseen ja tietoliikennelaitteisiin. Riskianalyysissa arvioidaan tietoturvauhkien todennäköisyyksiä ja niistä koituvia haittoja. Riskianalyysin avulla tietoturvasta aiheutuvat kulut pysyvät paremmin hallinnassa ja tietoturvan taso pysyy järkevänä. Äärimmäisen kireät säännöt eivät välttämättä palvele yrityksen tietoturvaa löysiä sääntöjä paremmin, jos asianomaisilla on hankaluuksia päästä tietoihin käsiksi. Edellä mainittujen toimien lisäksi yrityksen tietoturvan kannalta oleellinen asia on tietoturvaohjelmistojen ja tietokoneiden käyttöjärjestelmien pitäminen ajan tasalla.

## 3.2 Palomuurit

Palomuuri (firewall) on yhdistelmä aktiivilaitetta ja ohjelmistoa, jonka tarkoitus on rajata kahden tai useamman verkon välistä liikennettä sääntöihin perustuvien tietoturvakäytäntöjen avulla. Yleensä palomuurin toisella puolella on sisäverkko ja toisella Internet. Palomuuri voi toimia tietoliikenteen rajaamisen lisäksi proxy-, DHCP- tai NAT-palvelimena sekä VPN-yhdyskäytävänä.

Palomuurien avulla yritys pitää oman sisäverkkonsa erillään Internetissä. Ilman palomuureja tietoturvan tavoitteita ei voitaisi taata. Yrityksen verkkoresurssit olisivat kaikkien saatavilla, jos ulko- ja sisäverkon välistä liikenteen rajoitinta eli palomuuria ei olisi. Palomuuri voi olla erillinen laite, palvelin, reititin tai ohjelmisto. Yrityksissä voidaan käyttää näitä kaikkia yhdessä. Yksityisissä talouksissa tai pienissä verkoissa palomuurina toimivat yleensä ohjelmistopohjaiset palomuurit tai reititin. Myös palomuuriksi rakennettuja työasemia käytetään pienien verkkojen turvana.

Tavallisimpia käytössä olevia palomuureja ovat ns. pakettisuodatuspalomuurit(packet filtering). Pakettisuodatuspalomuureja on myös tilallisina (stateful). Palomuurit tuhoa-

vat kaikki palomuurien sääntöjä (filter rule tai ACL, Access Control List) rikkovat paketit. Säännöt perustuvat pakettien otsikkotietoihin. Näistä tiedoista nähdään paketin lähde- ja kohdeosoite, protokolla, paketin liput jne. Säännöistä riippuen kaikki nämä voidaan käydä läpi, ennen kuin paketin kohtalo on selvillä. Palomuurien rakennus tulisi aina aloittaa kieltämällä kaikki liikenne kokonaan. Tämän jälkeen voidaan alkaa lisätä tunnettuja ip-osoitealueita ja avata tarvittavia portteja. Paketin saapuessa palomuuriin, sitä verrataan järjestyksessä palomuurin sääntöihin, kunnes sopiva sääntö löytyy. Palomuuri toimii tämän jälkeen säännön mukaisesti. Säännöt ovat palomuurin tehokkuuden kannalta tärkeä asia, joten niiden luomisessa on syytä olla tarkkana. Säännöt on hyvä pitää mahdollisemman yksinkertaisina ja jokaisen säännön tulisi rajata liikennettä mahdollisemman paljon. Myös yrityksen sisäverkon koneilta lähtevää liikennettä on tärkeä rajoittaa (Troijan hevoset, p2p). Normaalien pakettisuodatuspalomuurien lisäksi on olemassa myös tilallisia palomuureja, jotka muistavat sen kautta kulkevan yhteyden tilan. Näin ollen palomuurin voi konfiguroida päästämään paketit suojattuun verkkoon vain, jos ne ovat suojatusta verkosta lähteneiden pakettien vastauksia. Tilallisen pakettisuodatuksen ansiosta ulkopuoliset koneet eivät voi avata yhteyttä suojatussa verkossa oleviin työasemiin. Pakettisuodatusta käyttävillä palomuureilla on kuitenkin heikkoutensa, joten yksinään ne eivät takaa yrityksen tietoturvallisuutta. Internet-liikenne portista 80 on palomuurin näkökulmasta harmitonta, mutta voi pitää sisällään haitallista tietoa. [7, s. 68 - 72]

Palomuuriin tulevasta liikenteestä pidetään yllä lokia. Lokitiedostojen avulla voidaan seurata palomuuriin saapuvaa liikennettä hyvinkin tarkasti. Näin palomuurin ylläpito helpottuu. Lokien avulla voidaan paikallistaa esim. tietoliikennelaitteissa olevia viallisia konfiguraatioita.

## 3.3 IDS

Palomuurien ohella tietoverkon suojana voi olla erillinen IDS-järjestelmä (Intrusion Detection System). Tällä järjestelmällä voidaan tunnistaa alkavia hyökkäyksiä ja toimia ennen kuin hyökkäyksestä koituu vaaraa suojatulle verkolle. IDS-järjestelmä käyttää hyväkseen hyökkäysmalleja etsiessään hyökkäyksen merkkejä (näitä voivat olla tietopakettien otsikkotiedoissa, tietyt bittijonot jne.). Yksi suosituimmista IDS-hyökkäysmallien jakelija on Snort (http://www.snort.org). Hyökkäys, joka saattaisi päästä läpi palomuurista, voidaan huomata IDS-järjestelmän avulla. Jokainen hyökkäyksen tunnuspiirteet omaava tapahtuma verkossa kirjataan IDS-lokiin. IDS-järjestelmän voi konfiguroida lähettämään sähköpostia verkon ylläpitäjille, jos tietyn tyyppisiä hyökkäyksiä esiintyy.

IDS-järjestelmiä on kahdenlaisia: verkkopohjainen IDS eli NIDS(Network-based IDS) ja tietokonepohjainen eli HIDS(host-based IDS). Verkkopohjainen IDS asennetaan yleensä tärkeään verkon osaan, jolloin IDS voi seurata verkon tietoliikennettä parhaiten. Tietokonepohjaiset IDS-järjestelmät seuraavat isäntäkoneen lokitiedostoja ja päättelevät niiden perusteella, onko kone hyökkäyksen kohteena.

Järjestelmällä on kuitenkin heikkouksia. Se on altis lähettämään paljon vääriä hälytyksiä, jos verkossa liikkuu paljon esim. ohjelmistovirheistä johtuvaa roskatietoa. Väärien hälytyksien suuri lukumäärä voi haudata oikeista hyökkäyksistä johtuvat hälytykset, jolloin niitä ei huomata. IDS-järjestelmää voidaan myös harhauttaa naamioimalla hyökkäys siten, ettei se vastaa enää totuttuja hyökkäysmalleja.[7, s. 86-94]

## 3.4 Yritysten virustorjunta

Palomuurit eivät yksin riitä suojaamaan yrityksen työasemien ja palvelimien turvallisuutta. Palomuurit eivät pysty suodattamaan pois Internet-liikenteen mukana tulevaa haitallista tietoa tai huomaamaan saastuneita liitetiedostoja sähköpostissa. Muun muassa näiden syiden vuoksi virustorjuntaohjelmisto on yrityksen tietoturvallisuuden ja toiminnan vuoksi tärkeää. Virusten leviämisen näkökulmasta vaarallisimpia ovat sähköpostit, käyttäjien tallennusmediat ja epäluotettavat Internet-sivut. Sähköpostin avulla leviäviä haittaohjelmia voidaan estää käyttämällä postinsuodatusta.

Isoissa yrityksissä virustorjuntaa voidaan hallita keskitetysti. Palvelimella toimiva hallintaosa määrää tietoverkon virustorjuntapolitiikat, joita verkon työasemat ja muut palvelimet noudattavat. Yleensä palvelimet ja työasemat on syytä jakaa omiin osioihinsa ja luoda näille omat virustorjuntapolitiikat. Keskitetty hallinta parantaa verkon turvallisuutta, sillä vakavat virustartunnat havaitaan helpommin ja saastunut kone saadaan pois verkosta nopeammin. Keskitetty hallinta helpottaa myös virustorjunnan ylläpitoa.

### 3.4.1 Virukset ja haittaohjelmat

Tietokonevirus on tietokoneelle haitallinen ohjelma, jotka kopioivat itseään. Tietokonevirukset leviävät yleensä isäntäohjelmien sisällä. Viruksen tartuttamia ohjelmia tai tiedostoja kutsutaan saastuneiksi. Ne voivat saastuttaa käytännössä jokaisen osan tietokoneesta aina käynnistystiedostoja ja BIOS:ia myöten. Virus ei voi levitä itsekseen, vaan tarvitsee aina ulkopuolisen tiedoston. Tietokonevirus voi aiheuttaa laajoja vahinkoja yrityksen tietojärjestelmissä. Tietokoneviruksia ilmestyy koko ajan lisää sitä mukaa, kun viruksentorjunta kehittyy. Viruksia on useita erilaisia. Näitä ovat esim. makrovirus, joka on vain muutaman koodirivin kokoinen tai polymorphiset virukset, jotka muuttavat koodiaan joka kerta saastuttaessaan tiedoston. Polymorphiset virukset ovat muuntautumiskykynsä ansiosta hyvin hankalia huomata.

Kuten tietokonevirukset, myös madot ovat tietokoneelle haitallisia ohjelmia. Virusten tapaan nekin kopioivat itseään, mutta toisin kuin virukset, ne eivät tarvitse toimiakseen isäntäohjelmaa. Madot voivat sisältää tietoverkon ja työaseman kannalta hyvinkin haitallista koodia, mutta yleensä matojen tarkoitus on ainoastaan levitä esim. sähköpostin välityksellä. Verkolle leviäminen aiheuttaa ongelmia, sillä saastuneet koneet kuormittavat verkkoa hyvinkin paljon, jolloin verkon normaali toiminta voi häiriintyä.

Troijan hevonen on haitallinen ohjelma, joka naamioituu hyödylliseksi ohjelmaksi levitäkseen. Yleensä nämä muka-hyödylliset ohjelmat tekevät aivan muuta kuin lupaavat. Ne voivat tuhota tai saastuttaa tiedostoja ja avata ns. takaportteja tietokoneeseen. Yleensä Troijan hevonen yrittää kerätä tietoa (esim. keylogger, joka kerää tietoa näppäimis-

töllä kirjoitetusta tekstistä) isäntäkoneestaan ja lähettää sen takaportin kautta eteenpäin. [7, s. 345 - 354]

### 3.4.2 Spy- ja Scareware

Spywarella tarkoitetaan ohjelmaa tai tekniikkaa, jolla koetetaan kerätä tietoa käyttäjästä ja tietokoneesta. Kerätyt tiedot lähetetään ohjelmassa tai koodissa määrättyyn osoitteeseen. Spyware yrittää asentua käyttäjän koneelle salaa ja pyrkii pysymään salassa. Spywarea voi asentua tietokoneelle jonkun toisen ohjelman mukana, ns. kylkiäisenä, se voi tarttua työasemaan Internet-sivuilta tai sähköpostista. Siitä voi olla jopa maininta asennettavan ohjelman asennuksessa, mutta se on hukutettu taitavasti esim. lisenssitekstin sekaan. Spyware ei itsessään ole haitallinen koneen toiminnan kannalta. Se eroaa viruksista ja muista haittaohjelmista siten, että se ei monista itseään tai aiheuta harmia isäntäkoneelleen. Tästä syystä varsinkin ilmaiset virustorjuntaohjelmat eivät aina huomaa spywarea. Maksulliset ja uudemmat virustorjuntaohjelmat pystyvät estämään spywaren leviämisen koneelle. Uudet virustorjuntaohjelmat pystyvät myös poistamaan havaitun spywaren. Hyvin harvoin poistaminen onnistuu normaalisti Windowsin avulla. Spyware tarttuu tietokoneisiin esim. Internet-sivujen, vertaisverkkojen tai ilmaisten ohjelmien välityksellä. Yrityksen tietoturvan kannalta spyware muodostaa selvän uhkatekijän. Levitykseen saattaa joutua käyttäjätunnuksia, salasanoja tai muuta arkaluontoista materiaalia, jolloin tietoturvan tavoitteet eivät enää täyty. Lisäksi spywaren saastuttama käyttäjä joutuu yleensä kestämään sähköpostin välityksellä tulevia mainoksia eli spämmiä. [8]

Scareware on lisääntynyt viime vuosien aikana huomattavasti. Scarewarella tarkoitetaan ilmaista hyötyohjelmaa (yleensä virustorjuntaohjelma tai vastaava tietoturvasovellus), joka on löytävinään käyttäjän koneelta viruksia tai muita haittaohjelmia. Ohjelmaa mainostetaan hyvin aggressiivisesti (pop-up ikkunat, valeskannaukset, pakotetut lataukset), jolloin käyttäjä voi tietoturvauhkien pelossa asentaa ohjelman. Todellisuudessa ohjelma joko valehtelee löydöistään tai pahimmillaan asentaa käyttäjän koneelle löytämänsä virukset ja haittatekijät. Scareware ilmoittaa pystyvänsä poistamaan haittaohjelmat, jos ohjelmasta ladataan maksullinen täysi versio. Kyseessä on siis huijausta tietoturvauhkien avulla.

Syksyllä 2009 tehtyjen löytöjen perusteella Internetistä löytyi yli 250 erilaista turvaohjelmaa, jotka täyttävät scarewaren tunnusmerkit. Arvioiden mukaan yli 40 miljoonaa käyttäjää on joutunut ohjelmien huijaamaksi vuonna 2008. Hankalaksi scarewaren tekee se, etteivät virustorjuntaohjelmat voi luokitella ohjelmia haitallisiksi. Syynä on se, että huijausohjelmien takana on yleensä laillinen yritys, joka puolustaa kaupallisia oikeuksiaan.

Yritysten kannalta scarewaresta voi muodostua ongelma. Esimerkiksi etäyhteyden avulla työskentelevä käyttäjä on erinomainen kohde scarewarelle. Varsinainen scareware ohjelma ei itsessään välttämättä ole ongelma yrityksen tietoturvan kannalta. Uhkana ovat ennemminkin ohjelman mahdollisesti asentamat oikeat haittaohjelmat, kuten virukset ja Troijan hevoset. Tehokas ratkaisu scarewaren välttämiseen on asennusoikeuksien rajoittaminen tietotekniikkatuelle ja henkilöstökoulutus yrityksen sisällä. [7, s. 226, s. 348][9]

## 3.5 Fyysinen tietoturva

Fyysinen tietoturva on yrityksen kannalta ainakin yhtä tärkeää kuin ohjelmistojen ja verkon ratkaisuilla saavutettu tekninen tietoturva. Fyysisellä tietoturvalla tarkoitetaan palvelimien, aktiivilaitteiden, työasemien ja näihin liittyvien resurssien turvaamista niin, etteivät asiattomat pääse niitä käyttämään tai varastamaan. Fyysiseen tietoturvaan kuuluu myös olemassa olevan tiedon suojaamista ulkopuolisilta haitoilta ja riskeiltä, kuten tulipaloilta ja sähkökatkoksilta. Fyysistä tietoturvaa arvioidessa on hyvä tehdä riskianalyysit kunkin uhkatekijän todennäköisyyksistä ja aiheutuvista haitoista. Riskianalyysin avulla yritys säästää resursseja ja kohdentaa ne oikeisiin asioihin.

Asiattomien pääsyä tietoon käsiksi ja verkkoon liittymistä yrityksen sisällä voidaan rajoittaa usein eri keinoin. Yleisimpiä keinoja ovat kulunvalvonta (kulkukortit), vartiointi ja hälytysjärjestelmät. Aktiivilaitteisiin ja palvelimiin sovelletaan tiukempaa kulunvalvontaa kuin normaaleihin työasemiin, mutta myös niihin pääsyä tulee rajoittaa. Yrityksen työkäytössä olevat työasemat on syytä pitää työhuoneissa ja ainoastaan henkilökunnalle tarkoitetuissa tiloissa. Hyvänä käytäntönä voidaan pitää sitä, ettei yrityksen julkisiin tiloihin asenneta työasemia, joilta on yhteys yrityksen muuhun verkkoon. Palvelimien ja aktiivilaitteiden sijainti yrityksessä on luottamuksellista tietoa eikä esim. jako-

kaappien ovissa kannata olla muuta kuin numeromerkintä. Palvelintiloihin pääsyä on syytä rajata, jotta vain yrityksen tietotekniikkatuella on pääsy niihin. Perusperiaatteena voidaan pitää sitä, että jokainen yrityksen työntekijä saa vain ne oikeudet, jotka tarvitsee työnsä tekemiseen. Virka-ajan ulkopuolella ja yrityksen ollessa suljettuna yrityksen tiloja on hyvä suojata hälytysjärjestelmällä ja vartioinnilla. Kulunvalvontaan voi liittyä myös lokien pito ovien avauksissa.

Verkkorasioiden sijoittelussa tulee ottaa huomioon, ettei yrityksen verkkoon pääse kytkeytymään kuka vain. Sijoittelussa on harkittava tarkoin, onko verkkorasioita järkevää viedä julkisiin tiloihin lainkaan. Yksi keino hankaloittaa luvatonta kytkeytymistä yrityksen sisäverkkoon on poistaa DHCP:n käyttö ja rajoittaa IP-osoitteiden käyttöä. Lisäksi rasioiden kytkennöissä on hyvä noudattaa periaatetta: jos rasiaa ei käytetä, ei sitä myöskään kytketä.

Ulkoisia uhkia, kuten tulipaloja ja sähkökatkoja varten on hyvä olla omat turvajärjestelmänsä. Palvelin- ja tiedonvarastointitiloissa on syytä olla hyvät sammutusjärjestelmät. Varavirran (varageneraattorit, UPS:it) käyttö palvelimissa auttaa sähkökatkoksia vastaan. Varmuuskopiot on syytä säilyttää eri tilassa kuin palvelimet ja alkuperäiset tiedot. Tulipalojen varalta varmuuskopiot ja muut tärkeät resurssit voidaan sijoittaa paloturvallisiin kaappeihin. Ulkoisilta uhkilta suojautuessa on kuitenkin muistettava, ettei turvallisuutta ylimitoiteta.

Palvelimien lisäksi tärkeät tietoliikennelaitteet on syytä suojata hyvin. Tärkeimmät kytkimet ja reitittimet voidaan pitää niille varatuissa tiloissa, jonne vain yrityksen tietotekniikkatuella on kulkuoikeudet. Yrityksen tiloissa olevat jakokaapit on pidettävä lukittuina. Jakokaapeissa olevat kytkimet on kuitenkin syytä suojata myös salasanoilla (kirjautuminen, hallintaportit jne.). Aktiivilaitteiden kirjautumisvaiheessa voidaan mainita konfiguroinnin olevan kielletty asiattomilta. Yrityksen oikeusturvan kannalta varoitustekstit ovat tärkeä asia. Tietoliikennelaitteiden turvaa edistävät myös tarpeettomien porttien ja palveluiden pois kytkeminen. [10]

Salaisten dokumenttien ja niitä sisältävien tallennusmedioiden kanssa on syytä olla tarkkana. Varsinkin USB-tikut, jotka sisältävät yrityksen kannalta salaista tietoa ovat

ongelmallisia tietoturvan kannalta. Ongelman voi osittain kiertää kryptaamalla yrityksen ulkopuolella liikkuvan salaisen tiedon. Salaisten dokumenttien hävityksestä on huolehdittava erikseen.

## 3.6 Käyttäjät ja tietoturva

Yrityksen tietoturvan kannalta suurin haaste ovat yrityksen verkkoa käyttävät työntekijät. Palomuurit, virustorjunta ja muut turvakeinot ovat kaikki ihmisten luomia ja näin ollen niissä on puutteita. Nämä turvatoimet eivät estä käyttäjää tuomasta haittaohjelmia henkilökohtaisella USB-tikulla käyttäjän kotikoneelta.

Mietittäessä yrityksen tietoturvastrategiaa on hyvä muistaa, että mitä pienemmillä oikeuksilla verkossa ja yrityksen järjestelmissä liikutaan, sitä turvallisempi ja helpompi se on hallita. Tämä tarkoittaa sitä, että jokaisella ohjelmalla, järjestelmällä ja käyttäjällä (järjestelmänvalvoja tai normaali käyttäjä) ovat vain ne oikeudet, joita ohjelma tai henkilö tarvitsee työnsä tai tehtävänsä suorittamiseen. Käytännössä normaalikäyttäjällä ei ole siis oikeuksia muuttaa työasemansa asetuksia eikä asentaa työasemalle mitään. Järjestelmänvalvojilla ei ole tunnuksia, jotka kävisivät jokaiseen verkon osaan ja joilla voitaisiin hallita koko verkon jokaista asiaa, vaan vastuu on jaettu useammalle käyttäjätunnukselle.

Edellä mainituilla toimilla rajoitetaan tehokkaasti tietoverkkoja uhkaavien ohjelmien tai henkiöiden aiheuttamia vahinkoja. Käyttäjien Internetistä ladatut haittaohjelmat ja virukset eivät pääse leviämään niin helposti, jos käyttäjällä ei ole oikeuksia esim. ajaa kuin Internet-selainta ja työhönsä käytettäviä ohjelmia. Käyttäjien aiheuttamaa tietoturvariskiä voidaan pienentää huomattavasti asianmukaisella koulutuksella ja huolehtimalla, että jokainen yrityksen työntekijä tietää pääsääntöisesti, mikä on kiellettyä ja sallittua yrityksen tietoverkkoa käytettäessä. Yleisinä ohjenuorina voi olla esim. koneiden lukitus, jos niitä ei käytä, julkisella paikalla ei työasioista jutella, henkilökohtaista tallennusmediaa ei käytetä sekaisin töissä ja vapaa-ajalla. Koulutuksella pienennetään riskiä joutumasta ns. social engineering:in uhriksi. Termillä tarkoitetaan sitä, että ulkopuolinen henkilö soittaa tai ottaa muuten kuin kasvotusten yhteyttä työntekijään tekaistuilla tiedoilla. Yleensä hyökkääjä voi esiintyä tietyntason johtajana tai tietotekniikkatuen jäsenenä. Hyökkääjä pyytää käyttäjää kertomaan salasanansa tai vaikka asettamaan sen

tietyksi esim. huoltotoimenpidettä varten. Jos hyökkääjä on riittävän vakuuttava ja auktoriteetilta kuulostava, usein salasana onnistutaan ryöstämään. [6, s. 97 - 110]

# 4 TIETOTURVARAPORTIN LAATIMINEN JA PALVELIMIEN TIETOTURVAN KARTOITUS

## 4.1 Projektin lähtökohdat ja aloitus

Projektin tavoitteena on kartoittaa jokaisen PSSHP:n käyttämän palvelimen tietoturvataso sekä kartoittaa mahdolliset riskikäyttäjäryhmät ja niiden oikeudet palvelimiin. Projektia varten tehtyjen päätösten mukaan alustavien kartoituksien jälkeen palvelimia tarkastettaisiin säännöllisesti, jotta tietoturvataso pysyisi mahdollisimman korkealla. Palvelimia alettaisiin kartoittaa hiljalleen muiden töiden ohella, kun projektille tarpeelliset pohjatyöt olisi saatu tehtyä. Tämän opinnäytetyö keskittyy näihin pohjatöihin.

Palvelimien kartoitukset tehtiin pääasiassa Tenablen valmistamalla Nessus-tietoturvaskannerilla. Projektin alkaessa Nessus-tietoturvaskannerin uusin ja projektin alkuvaiheessa käytössä ollut versio oli 4.0.2. Ohjelma on yleisesti käytetty tietoturvaskanneri, jonka avulla etsitään tietoturva-aukkoja tietoverkon työasemista ja palvelimista. Käyttäjäryhmien kartoituksiin käytetty ohjelma valittiin opinnäytetyön aikana. Ohjelman vaatimuksiksi asetettiin se, että sillä pystyttiin raportoimaan tiettyjen käyttäjäryhmien oikeudet yksittäisien palvelimien jakoihin ja paikallisiin resursseihin. Lisäksi ohjelman tuli olla ilmainen tai kunnollisen kokeiluosuuden sisältävä. Tuotantokäytössä olevaa ISA-julkaisupalvelinta ei kartoitettu palvelimen luonteen ja ajan niukkuuden vuoksi.

Projektissa työskenteli alussa pääsääntöisesti ainoastaan opinnäytetyön tekijä. Vetäjänä toimi järjestelmäinsinööri Marko Ruotsala, joka myös teki lopulliset päätökset projektin tuotantoverkkoa koskevista asioista. Lisäksi projektiin osallistui hetkellisesti henkilöitä palvelin- ja tietoliikenneyksiköstä, kun ISA-julkaisupalvelimen kartoittamista suunniteltiin.

## 4.2 Projektin suunnitteluvaihe

Projekti aloitettiin virallisesti 11.11.2009, kun opinnäytetyötä varten tarvittava aloituspalaveri oli pidetty. Tätä ennen projektia varten oli tehty taustatyötä tutustumalla PSSHP:n käytössä oleviin palvelimiin ja katsottu alustavat testipalvelimet, joihin opinnäytetyön kartoitukset tehtäisiin. Näiden alustavien toimenpiteiden lisäksi kaikista käytössä olevista Windows-palvelimista oli kerätty tietoa paikallisista käyttäjistä ja ryhmistä. Tätä tietoa voitaisiin hyödyntää projektin edetessä. Projektia edeltäviin pohjatöihin kuului riittävien oikeuksien myöntäminen opinnäytetyön tekijälle, jotta projektin vaatimat työt saataisiin tehtyä. Pohjatyöt projektia varten tehtiin lokakuun 2009 aikana, jonka jälkeen projektin varsinainen suunnitteluvaihe voitiin aloittaa. Työn suunnitteluun ja toteutukseen saatiin melko vapaat kädet.

Projektin aloitus jaettiin seuraaviin vaiheisiin: suunnittelu ja aloitus, ohjelmien käyttöönotto ja testaus, tietoturvakartoitukset, raportointipohjan luonti ja testiraporttien laadinta. Kokonaisuudessaan näihin vaiheisiin käytettiin aikaa noin puolitoista kuukautta, mikä asetti varsinkin ohjelmien käyttöönotossa haasteita. Suunnitteluun tästä ajasta oli varattu pohjatöiden alettua noin kaksi viikkoa. Projektin aikana suoritetut tietoturvakartoitukset oli määrä saada valmiiksi joulukuun 2009 alkupuolella, jonka jälkeen raporttipohjan laadinnalle ja tuloksien raportoinnille jäi joulukuun 2009 loppu.

Suunnitteluvaihe aloitettiin kokoamalla testityöasema, jolta kaikki tulevat tietoturvakartoitukset tehtiin. Tähän työasemaan asennettiin KYS:n normaali työasemapaketti, mikä liitettiin tuotantoverkkoon, jolloin koneelta saatiin yhteys PSSHP:n sisäverkossa oleviin koneisiin ja palvelimiin. ISA-julkaisupalvelimen kartoitusta varten projektin käyttöön varattiin myös KYS:n etätyöasemapaketilla varustettu kannettava tietokone ja mobiililaajakaistaliittymä, jotta ISA-palvelinta voitiin tarkastella ulko- ja sisäverkosta käsin.

Suunnitelmien mukaisesti tietoturvakartoitukset tehtäisiin Nessus-ohjelmalla (http://www.nessus.org). Projektin menestyksellistä läpivientiä varten tarvittiin lisäksi ainakin yksi ohjelma, jolla käyttäjäryhmien kartoitus onnistuisi. Marko Ruotsalan ehdotuksen mukaisesti myös Microsoftin omaa skannausohjelmaa, Microsoft Baseline Security Analyzer testatiin. Ohjelmien käyttöönotto aloitettiin tutustumalla ohjelmien ohje-

kirjoihin ja käyttöoppaisiin. Tämän jälkeen ohjelmat asennettiin testikoneelle ja niiden testaaminen aloitettiin. Ensimmäisien testien aikana testikone kytkettiin pois verkosta, jotta ohjelmien aiheuttamat mahdolliset häiriöt tuotantoverkkoon saatiin estettyä. Ohjelmistot otettiin käyttöön seuraavanlaisessa järjestyksessä: Ensimmäiseksi testattiin Microsoftin Baseline Security Analyzer, tämän jälkeen Nessus 4.0.2 ja viimeisenä käyttäjäryhmien kartoitukseen käytettävän ohjelman valitseminen ja testaaminen.

Käyttöönottoa jatkettiin näiden vaiheiden jälkeen kytkemällä testikone verkkoon. Testikone A oli ensimmäisten verkon yli tehtyjen kartoituksien kohde. Näin varmistettiin, että ohjelmien avulla saatiin tietoa myös verkon yli. Viimeisenä vaiheena olivat kohdepalvelimien kartoitukset testikoneelta käsin. Marko Ruotsalan kanssa sovittiin, että kutakin sisäverkon testipalvelinta tarkasteltiin Nessus-ohjelmalla kaksi kertaa. Sisäverkosta tehdyt kartoitukset riittivät näihin palvelimiin, koska ne eivät ole julkisia eivätkä siten näy ulkoverkkoon. Ensimmäisellä kerralla kohdepalvelinta tarkasteltiin ilman Windows-tunnuksia ja toisella tarkastuskerralla Nessukselle annettiin toimialueen pääkäyttäjän oikeudet kohdepalvelimeen. Kahdella erilaisella kartoituksella kohdepalvelimen tietoturvasta saatiin eheämpi ja tarkempi kuva.

## 4.3 Tietoturvakartoituksissa käytetyt sovellukset

Projektin aikana käytettiin useita eri ohjelmia palvelimien tietoturvan määrittämiseen. Ohjelmistojen käyttöönotto aloitettiin tutustumalla ensimmäiseksi ohjelmien käyttöoppaisiin, jotta käsitys käytettävistä ohjelmista paranisi eikä ohjelmiin tutustumiseen tarvitsisi käyttää niin paljon aikaa. Ohjeisiin tutustumisen jälkeen aloitettiin ohjelmien asennus.

### 4.3.1 Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer-työkalu on Microsoftin kehittämä tietoturvatyökalu, jolla voidaan suorittaa tietoturvakartoituksia paikallisesti tai verkon yli. Ohjelmal-

la voidaan kartoittaa Windowsien tietoturvan lisäksi mm. IIS ja Internet Explorerin tietoturvaa. Ohjelmalla saadaan selville mm. tietoturvapäivityksien puutteet.

Ohjelmaa ajettaessa testikoneessa kävi kuitenkin ilmi, ettei tällä ohjelmalla palvelimien kartoitus tällä ohjelmalla olisi kovinkaan mielekästä tai järkevää. Ohjelma itsessään kartoittaa vain tiettyjen Microsoftin omien ohjelmien tietoturvatasoa eikä puutu lainkaan muihin ohjelmiin tai epäkohtiin. Projektin tarkoitus oli selvittää, löytyykö PSSHP:n käyttämistä palvelimista tietoturva-aukkoja, joita voidaan käyttää hyväksi ilman asianmukaisia tunnuksia. MSBSA:lla tätä ei voitaisi selvittää. Tämä tarkoittaa sitä, etteivät esim. Javan tai muiden ohjelmien muodostamat tietoturva-aukot näy testien tuloksissa. MSBSA:ta ei käytetty projektin edetessä tietoturvakartoitus-vaiheeseen.

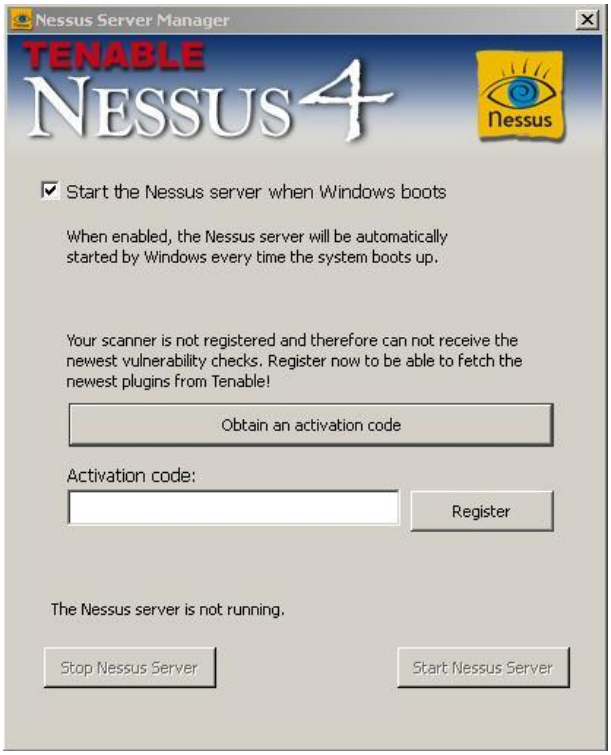
### 4.3.2 Nessus 4.0.2 ja sen käyttö projektin aikana

Tenablen valmistama Nessus-tietoturvaskanneri on yksi maailman käytetyimpiä tietoturvaskannereita, ja sitä käytetään ympäri maailmaa erilaisissa ja erikokoisissa yrityksissä. Se on alun perin UNIX-maailmasta lähtöisin oleva tietoturvaskanneri, mutta sitä saa myös Windows-versiona. Nessus 4.0.2:sta on olemassa myös MAC OS X:lla toimiva versio. Aiemmin mainitun tietoturvaraportin perusteella tätä ohjelmaa käytettiin myös tämän projektin aikana ja sillä hoidettiin palvelimien tietoturvakartoitukset.

Projektin aikana käytettiin Nessus 4.0.2 -versiota, joka oli projektin alussa uusin mahdollinen versio. Opinnäytetyön lopussa ilmestyi uusi versio 4.2, joka eroaa ulkoasultaan 4.0.2:sta paljon. Opinnäytetyön aikana käytetty versio oli Nessus 4.0.2. Ohjelma vaatii toimiakseen ns. Nessus-palvelimen ja Nessus-asiakaspään. Nessus toimii siten, että asiakaspään ohjelma eli Nessus-client ottaa yhteyttä Nessus-palvelimeen, jonka avulla kartoitukset tehdään. Opinnäytetyön kannalta oli helpotus, että Nessus-clientin ja Nessus-serverin pystyi asentamaan samalle koneelle. Työn aikana näitä molempia ajettiin samalta testikoneelta.

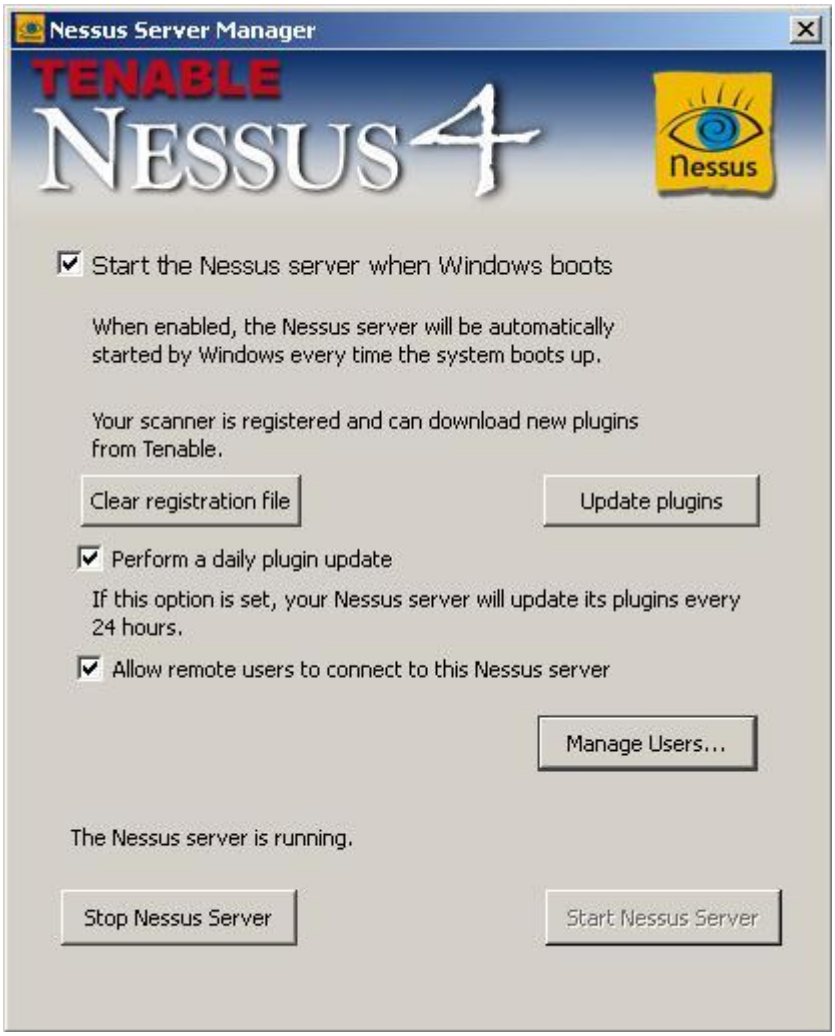
Nessuksen asennuksen jälkeen ohjelma täytyy rekisteröidä ja aktivoida.. Aktivointivaiheessa päätetään, otetaanko käyttöön ilmainen vai laajempi ja maksullinen versio ohjelman käyttämistä kartoitusliitännäisistä (plug-in). Projektin alkuvaiheessa ja opinnäy-

tetyön aikana ilmainen versio oli asetettujen tavoitteiden saavuttamiseksi riittävä. Ilmaisen ja maksullisen version erona on se, että maksullinen tarjoaa parempaa asiakastukea ja auditointityökaluja. Projektissa tultaisiin toimeen ilman niitä. Aktivointi tapahtuu seuraamalla ohjelman antamia ohjeita, kun se käynnistetään ensimmäisen kerran (kuva 1).




**Kuva 1. Ohjelman ensimmäinen käynnistys ja kehotus aktivoida tuote.**

Aktivointikoodi saatiin rekisteröinnin jälkeen ohjelman kotisivulle jätettyyn sähköpostiosoitteeseen. Jokainen uusi Nessus-ohjelman asennus vaatii oman aktivointiavaimensa, joten myös projektin käytössä olleeseen mobiililaajakaista-koneeseen asennettiin Nessus samalla kertaa. Aktivoinnin jälkeen ohjelman aloitusikkuna näyttää kuvan 2 kaltaiselta.

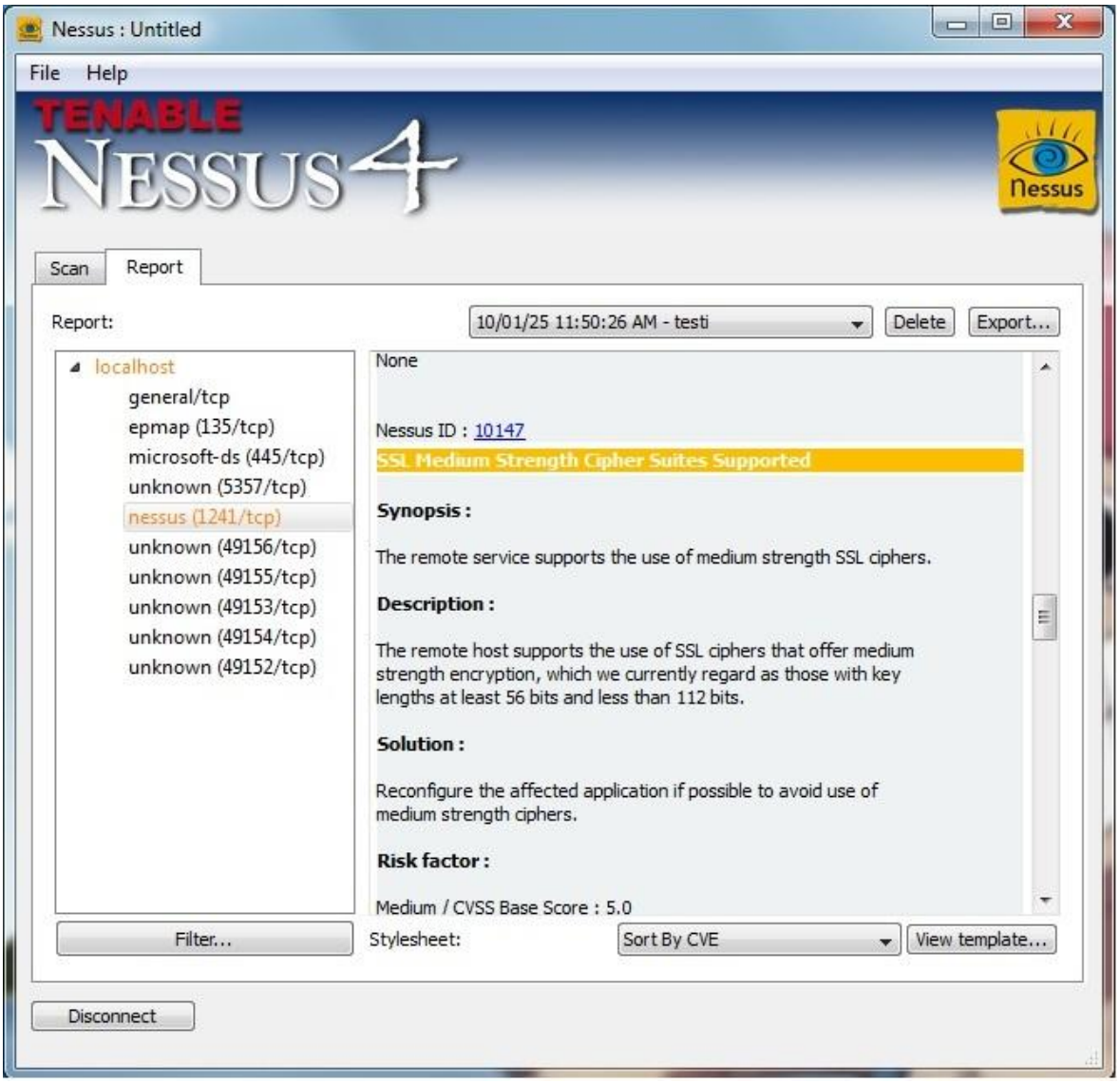



**Kuva 2. Nessus-ohjelman aloitusikkuna aktivoinnin jälkeen.**

Nessus-server:in ollessa pystyssä, koetettiin client-osalla ottaa yhteyttä samalla työasemalla olevaan palvelimeen. Ohjelman käyttö oli verrattain helppoa, mikä oli projektin kannalta erinomainen asia. Clientin toiminta varmistettiin asettamalla tietoturvakartoituksen kohteeksi ip-osoite 127.0.0.1 eli paikallisen työaseman (localhost) osoite.

Jotta kartoitus onnistuisi, piti Nessuksella luoda ns. skannauspolitiikka, jossa määriteltiin tietoturvakartoitukseen käytettävät liitännäisosat, tietoverkon kuormittamiseen liittyvät asetukset ja mahdolliset käyttäjätunnukset esim. Windows-käyttöjärjestelmää varten. Säädettäviä ominaisuuksia on ohjelmassa valtavasti. Opinnäytetyön kannalta kaikkien erilaisten asetuksien kokeileminen todettiin tarpeettomaksi, sillä tarkoitus oli saada hyvä yleiskuva palvelimien tietoturvasta. Vaikka ohjelman lisäasetuksista löytyi useita hyvinkin mielenkiintoisia testejä, kuten mahdollisten heikkouksien rasitus ja yritys kaataa kohdekoneelta prosesseja, oli muistettava, että kyseessä on sairaalan tuotantoverkko. Näistä syistä johtuen päätettiin käyttää oletusasetuksia ja jättää mahdolliset rasitustestit ja kokeellisia hyökkäyksiä testaavat ajot pois. Ainoat muutokset kartoitusasetuksiin olisivat eri Windows-käyttäjätunnukset. Testikone kytkettiin pois verkosta varmuuden vuoksi ennen kuin kartoitus aloitettiin, ettei koituisi ikäviä yllätyksiä.

Testikonetta tarkasteltiin kaksi kertaa. Toisella kerralla käytössä oli toimialueen pääkäyttäjän tunnukset. Tarkoitus oli verrata näiden kahden kartoituksen tuloksia ja etsiä eroavaisuuksia ja miettiä niiden merkitystä testikoneenkin kannalta, vaikkei se kuulunutkaan raportoitavien koneiden joukkoon. Näin varmistettiin, että ohjelma toimi varmasti halutulla tavalla ja saadut tulokset olivat luotettavia. Paikalliseen testikoneeseen tehtyjen kartoituksien jälkeen ohjelma antaa kuvan 3 kaltaisen näkymän testituloksista.




**Kuva 3 Esimerkki paikalliseen testikoneeseen tehdystä tietoturvakartoituksesta**

Seuraavana projektinvaiheena oli liittää testikone takaisin verkkoon ja testata ohjelman ajoa verkon yli vieressä olevaan työasemaan. Työasemaa tarkasteltiin täysin samoilla asetuksilla kuin testikonetta. Saadut tulokset osoittivat, että kohdekoneista saatiin järkevää tietoa riippumatta siitä, tarkasteltiinko niitä Windows-käyttäjätunnuksien avulla vai ei. Työasemalle ja testikoneelle ajettiin läpi vielä muutamia testejä. Näillä testeillä haluttiin selvittää, paljonko kartoitukseen kuluisi enemmän aikaa, kun käytössä oli verkon kannalta kevyemmät asetukset. Todettiin, ettei yksittäistä konetta tarkasteltaessa eroa voinut huomata. Ohjelman antama tieto todettiin järkeväksi ja riittäväksi projektin tarpeisiin ja onnistuneiden testiajojen jälkeen oltiin valmiita siirtymään testipalvelimien kartoitukseen.

### 4.3.3 Testipalvelimien tarkastelu Nessus 4.0.2 -ohjelman avulla

Onnistuneiden testien jälkeen voitiin projektissa siirtyä palvelimien kartoittamiseen. Marko Ruotsalan antaman palvelinlistan mukaisesti tietoturvakartoitukset aloitettiin ennalta sovitusta testipalvelimesta. Mikäli kartoitukset tähän palvelimeen onnistuisivat suunnitelmien mukaisesti, siirryttäisiin kartoittamaan muita testipalvelimia. Osa näistä palvelimista sijaitsisi eri toimialueella kuin käytössä ollut testikone. Tällä tavoin saataisiin myös varmistettua, että toimialueitten yli tapahtuva kartoitus onnistuisi ilman ongelmia. Kaikki tässä dokumentissa tarkastellut testipalvelimet olivat Windows Server 2003 tai Windows Server 2008 -käyttöjärjestelmiä käyttäviä palvelimia ja kaikki niihin ajetut tietoturvakartoitukset tehtiin Windows XP -työasemalta käsin.

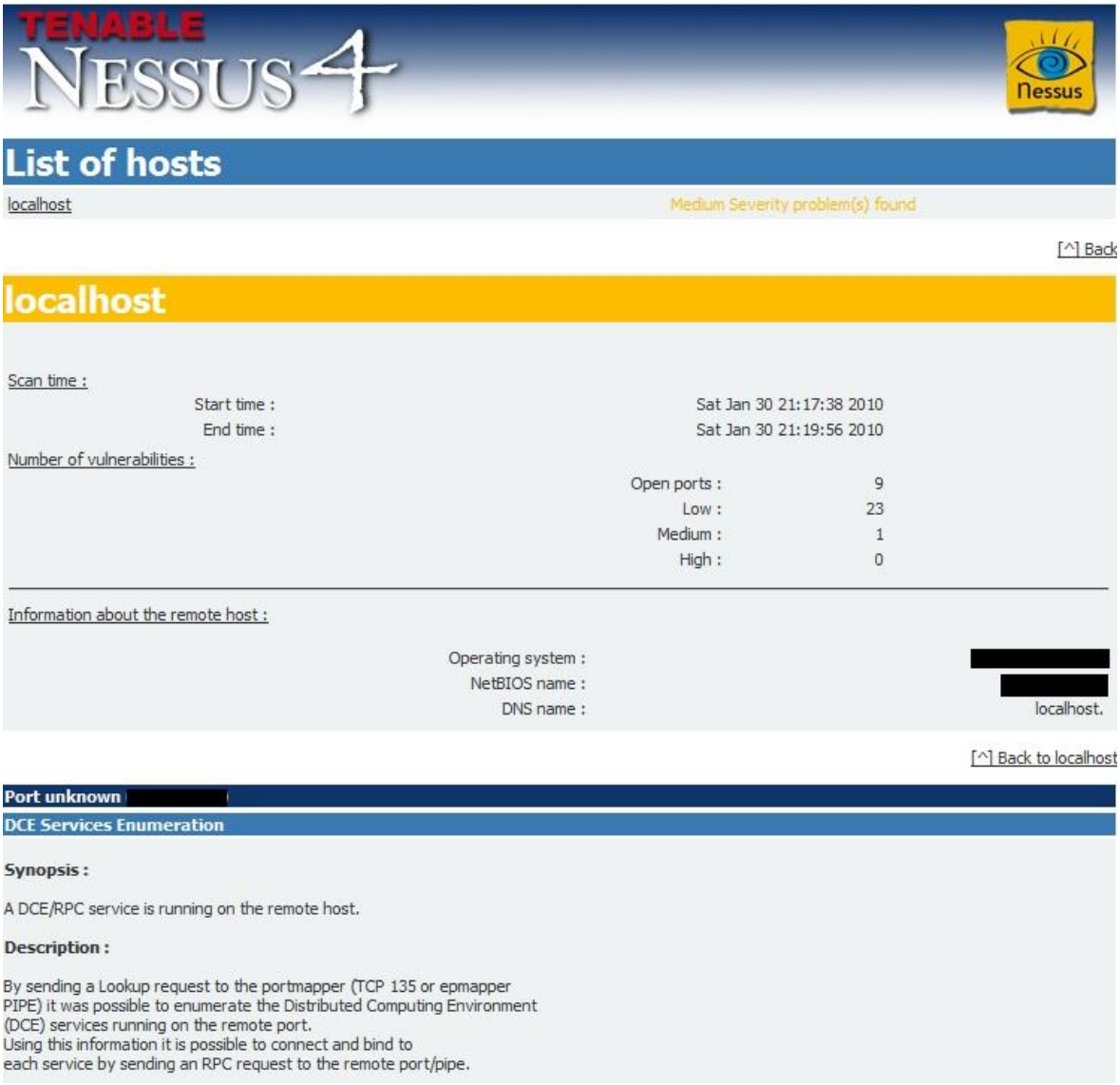
Testipalvelimeen kohdistuvia kartoituksia varten tehtiin muutamia toimenpiteitä ennalta käsin. Ennen kartoituksia varmistettiin, että testikoneelta saatiin etäyhteys kohdepalvelimeen. Samalla varmistettiin se, että pystyttiin käyttämään pääkäyttäjätason kirjautumistunnuksia ja ettei kyseinen palvelin ollut käytössä. Nämä samat ennakkotoimenpiteet tehtiin kaikille sisäverkon testipalvelimille. ISA-julkaisupalvelimelle tehtiin hieman eri valmistelut ja niistä kerrotaan myöhemmin tässä luvussa. Kun ennakkovalmistelut oli tehty, voitiin tietoturvakartoitukset aloittaa.

Testipalvelimia tarkasteltiin Nessuksen avulla ilman tunnuksia ja pääkäyttäjän tunnuksilla. Nessuksella ajettavat testit olivat käyttäjätunnuksia lukuun ottamatta perusasetuksilla. Näin saatiin jokaisesta testipalvelimesta tietoa samoilla ehdoilla ja saatuja tietoja voitiin vertailla helpommin. Toinen tietoturvakartoitus ajettiin Windows-tunnuksilla, jotta asennettujen ohjelmien ja käyttöjärjestelmän heikkoudet saatiin selville. Ohjelmien ja käyttöjärjestelmän heikkouksia ei voitu selvittää ilman käyttäjätunnuksien käyttöä. Sisäverkon testipalvelimien kartoitukset sujuivat suunnitelmien mukaisesti.

Projektin aikana tehtävien tietoturvaraporttien kannalta Nessus helpotti urakkaa huomattavasti, koska kohdepalvelimista saadut tulokset pystyi muuttamaan html-muotoiseksi raportiksi (kuva 4). Näistä raporteista saatiin helposti projektin kannalta kiinnostavat tiedot tietoturvaraportteihin. Nessus antoi ensin yhteenvedon kohdepalvelimesta. Näin voitiin nopeasti todeta kohdepalvelimen tietoturvataso. Raportissa käydään läpi jokai-

nen Nessuksen ilmoittama epäkohta tai riski. Jokaisesta palvelimesta otettiin kaksi html-raporttia.

Raporttiin tulevaa tietoa voitiin myös rajata suodattimien avulla. Ensimmäisestä tietoturvakartoituksesta luotiin Nessuksella raportti, jossa on esitetty kaikki kohdepalvelimesta löydetyt riskit. Raporttia läpikäytäessä huomattiin, että tietoa tuli valtavasti eikä kaikki esitetty tieto ollut projektin kannalta mielekästä. Nessus luokittelee löydetyt uhkatekijät kolmeen eri luokkaan: matala, keskitaso ja korkea. Matalan tason riskitekijät olivat usein palvelimista tietoa kerääviä (esim. mikä käyttöjärjestelmä). Raporteista päätettiin suodattaa pois kaikki matala-luokan riskitekijät, jotta oikeasti vaaralliset löydöt eivät hukkuisi Nessuksen tuottamaan tietotulvaan. Raportit palvelivat näin paremmin projektin tarpeita, kun niistä saatiin selkeä kuva kohdepalvelimen mahdollisista tietoturvaongelmista. Jokaisesta sisäverkon testipalvelimesta luotiin kaksi html-raporttia, joista jokaisesta oli suodatettu pois alimman tason ongelmat. Testipalvelimien kartoituksien aikana alettiin katsoa sopivaa ajankohtaa ISA-julkaisupalvelimen kartoitusta varten.




**Kuva 4. Esimerkki Nessuksen luomasta html-raportista.**

.

### 4.3.4 ISA-palvelimen tietoturvakartoitus Nessus 4.0.2:lla

ISA-julkaisupalvelimen tietoturvakartoitusta varten jouduttiin tekemään enemmän pohjatöitä kuin muiden testattujen koneiden kanssa. Kyseessä oli tuotantokäytössä oleva julkinen palvelin, jota ei voitu kartoittaa ilman asianmukaista tietoverkkokatkosta. Palvelimen tarkastelusta teki projektin kannalta mielenkiintoisen sen roolin lisäksi ISA-palvelimen oman palomuurin toiminta. Tietoverkkokatkoksesta huolehti järjestelmäinsinööri Marko Pursiainen yhteistyössä tietoliikenne- ja sovellusyksikön kanssa. Katkoksesta ilmoitettiin myös Kuopion kaupungin Atk-keskukselle. Näin mittavat valmistelut yhden palvelimen kartoitusta varten olivat tarpeen, koska kyseessä oli varsin kriittinen

palvelin. Palvelin oli osa tuotantoverkkoa, joten siihen kohdistuvat simuloidut hyökkäykset Nessuksella voisivat pahimmassa tapauksessa aiheuttaa häiriöitä verkkoon. Valmisteluilla pyrittiin minimoimaan tietoturvakartoituksen vaikutukset muuta verkkoa kohtaan.

ISA-julkaisupalvelinta oli alkuperäisten suunnitelmien mukaan tarkoitus tarkastella kaksi kertaa. Toinen näistä tarkasteluista suoritettaisiin projektin tarpeisiin varatulla mobiililaajakaistatietokoneella, jolloin tarkastelu tapahtuisi ulkoverkosta päin. Kartoituksessa ei käytetty käyttäjätunnuksia, jotta kartoituksien tulokset vastisivat parhaiten ulkopuolelta tapahtuvaa hyökkäystä. Suunnitelmiin tuli kuitenkin muutos jo olemassa olevien tietoturvaratkaisujen vuoksi. Ongelma varmistettiin, kun palvelimelle saapuvaa tietoliikennettä tarkkailtiin koko tietoturvakartoituksien ajan. Ongelman selvittyä kehitettiin yhdessä Marko Pursiaisen ja tietoverkkoyksikön Urpo Hämäläisen kanssa varasuunnitelma. Testikone päätettiin liittää suoraan samaan verkkoon kuin ISA-palvelin. Näin pystyttiin tarkastelemaan kohdepalvelimen tietoturvatasoa suoraan, eikä muita erikoisjärjestelyjä jouduttu tekemään. Kun tietoturvakartoitukset olivat ohi, liitettiin testikone takaisin sen omaan verkkoalueeseen. Vaikka alkuperäiseen suunnitelmaan kuulunut ulkoverkosta tuleva tarkastelu ei onnistunut, voitiin ISA-palvelimen tietoturvakartoitusta pitää onnistuneena, sillä varasuunnitelman mukaisella kartoituksella saatiin selville kohdepalvelimen tietoturvan taso ilman muiden muuttujien tai tekijöiden vaikutusta. Kohdepalvelimesta saatiin Nessuksen avulla irti järkevää tietoa. Näin voitiin tehdä johtopäätökset palvelimen tietoturvatasosta.

### 4.3.5 Palvelimien riskiryhmien kartoitukseen tarvittavan ohjelman etsintä

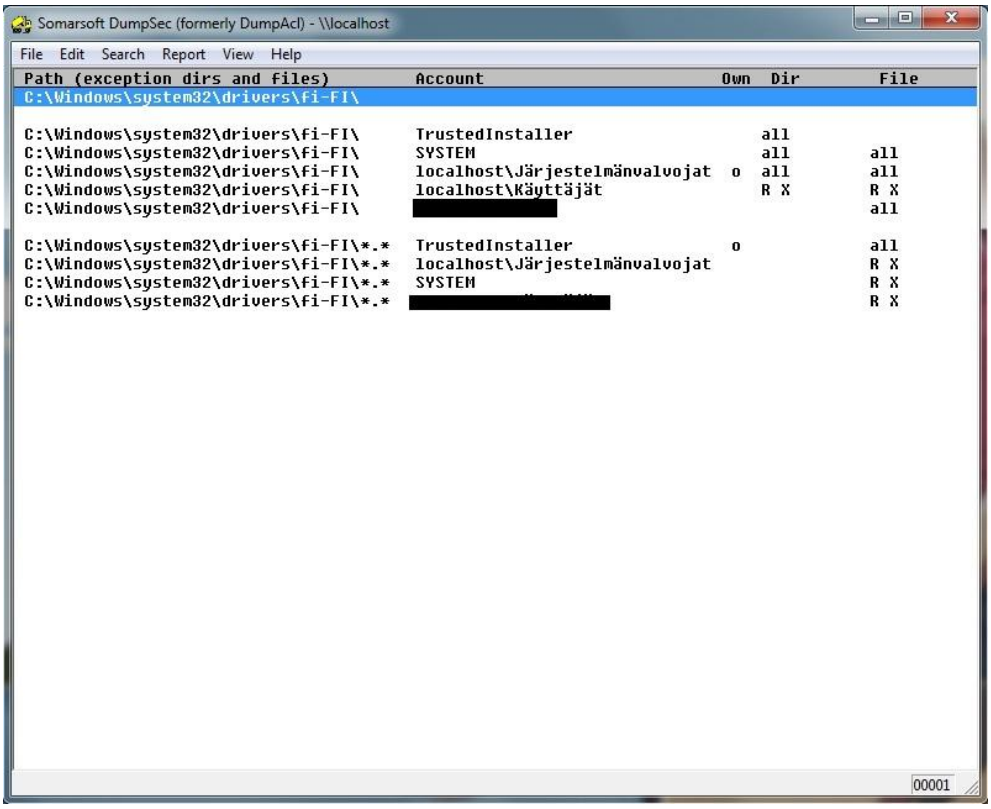
Projektin toinen osuus oli etsiä ohjelma käyttäjäryhmien oikeuksien kartoituksiin. Kohteena olivat erityisesti tiedostojaot ja kansiot, joihin Kaikki-ryhmällä oli täydet oikeudet. Tuotantoverkon tietoturvan kannalta näiden selvittäminen on ensisijaisen tärkeää. Kohdepalvelimilla saattoi olla tietoa, johon tavallisilla käyttäjillä ei pitäisi olla pääsyä lainkaan. Näitä ovat esimerkiksi tiedostot tai dokumentit, joita ei ole tarkoitettu kaikkien nähtäväksi tai muokattavaksi. Tavallisia käyttäjiä vaarallisempi tekijä on tietokoneviruksen aiheuttama uhka. Virus pystyy helposti saastuttamaan palvelimella olevat tiedot,

joihin Kaikki-ryhmällä on täydet oikeudet. Palvelimen saastutettuaan virus voisi aiheuttaa pahimmillaan mittavia tuhoja tuotantoverkkoon ja hankaloittaa sairaalan toimintaa.

Ohjelman etsimiseen ja oikeuksien kartoittamiseen saatiin Marko Ruotsalalta melko vapaat kädet. Kartoitukset tehtiin samoihin testipalvelimiin kuin Nessuksella tehdyt tietoturvakartoituksetkin. Ainoana erona oli se, ettei ISA-palvelimen oikeuksia kartoitettu opinnäytetyön aikana. Tarvittavien tietojen keruun pystyi luultavasi hoitamaan ilman erityistä ohjelmaakin käyttämällä skriptejä ja komentokehoitteen komentoja. Opinnäytetyön tekijälle ei ollut kuitenkaan tarpeeksi osaamista tähän ja ajan niukkuuden vuoksi sitä ei pidetty mielekkäänä vaihtoehtona. Päätettiin etsiä ohjelma, joka toimi Windows XP-käyttöjärjestelmässä ja jolla pystyttiin saamaan edellä mainitut tiedot kohdepalvelimista.

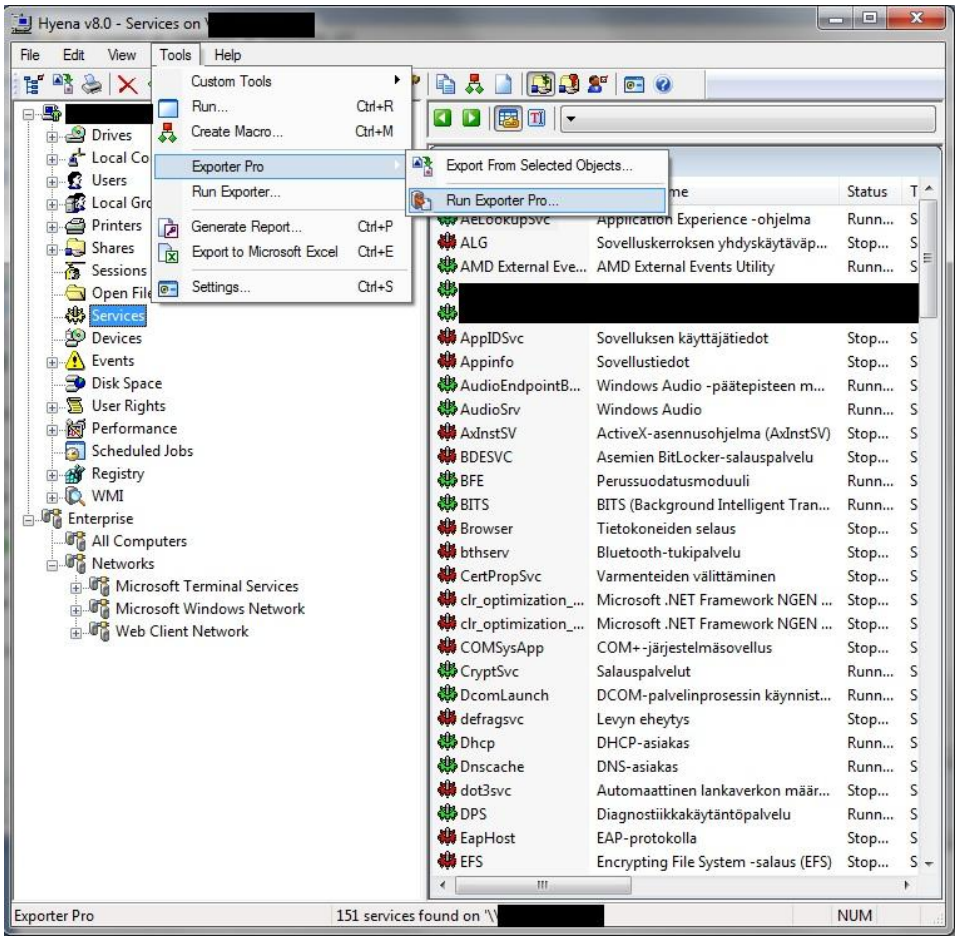
Ohjelman etsiminen aloitettiin käyttämällä Internetin eri hakukoneita (Google, Altavista) ja etsimällä asiaan liittyviä keskusteluja eri tietotekniikan keskustelupalstoilta. Sopivan ohjelman löytyminen hakukoneiden avulla oli toivottavaa projektin etenemisen kannalta. Internetistä löydettiin muutamia sopivia ehdokkaita. Testiin otetut ohjelmat olivat DumpSec ja Hyena (http://www.systemtools.com/somarsoft/?somarsoft.com), sekä Remote PC Tools, Oy:n valmistama PC Remote Permission Audit eli PCRPA (http://www.remotepctools.com/pc_remote_permissions_audit/features.html). Kukin näistä ohjelmista oli saatavana ilmaisena kokeiluversiona, joten ne ladattiin valmistajien kotisivuilta testikoneelle. Ohjelmien lataamisen yhteydessä koetettiin Internetin hakukoneilla löytää lisätietoa kustakin ladatusta ohjelmasta.

Ensimmäisenä testattiin DumpSec-ohjelmaa. Testissä selvisi nopeasti, että kyseessä on vanha ja käyttöliittymältään varsin yksinkertainen ohjelma. Testeissä kävi ilmi, että ohjelmalla pystyi selvittämään käyttäjäoikeudet paikallisen koneen tiedostoihin ja kansioihin (kuva 5). Ohjelman rajoitukseksi muodostui kuitenkin saadun tiedon suodatus. Projektin kannalta kiinnostavien ryhmien oikeuksien suodatus ei onnistunut ja PSSHP:n tuotantoverkon kokoisen verkon käyttäjäryhmiä ei ole mielekästä listata ilman tiedon suodatusta. Ohjelma tarjosi kyllä tietoa, mutta sitä oli näennäisesti mahdotonta lajitella, joten DumpSec:in käytöstä luovuttiin. Ohjelman läpikotaisin opettelu ei ollut opinnäytetyön puitteissa mahdollista, joten siirryttiin testaamaan Hyenaa.



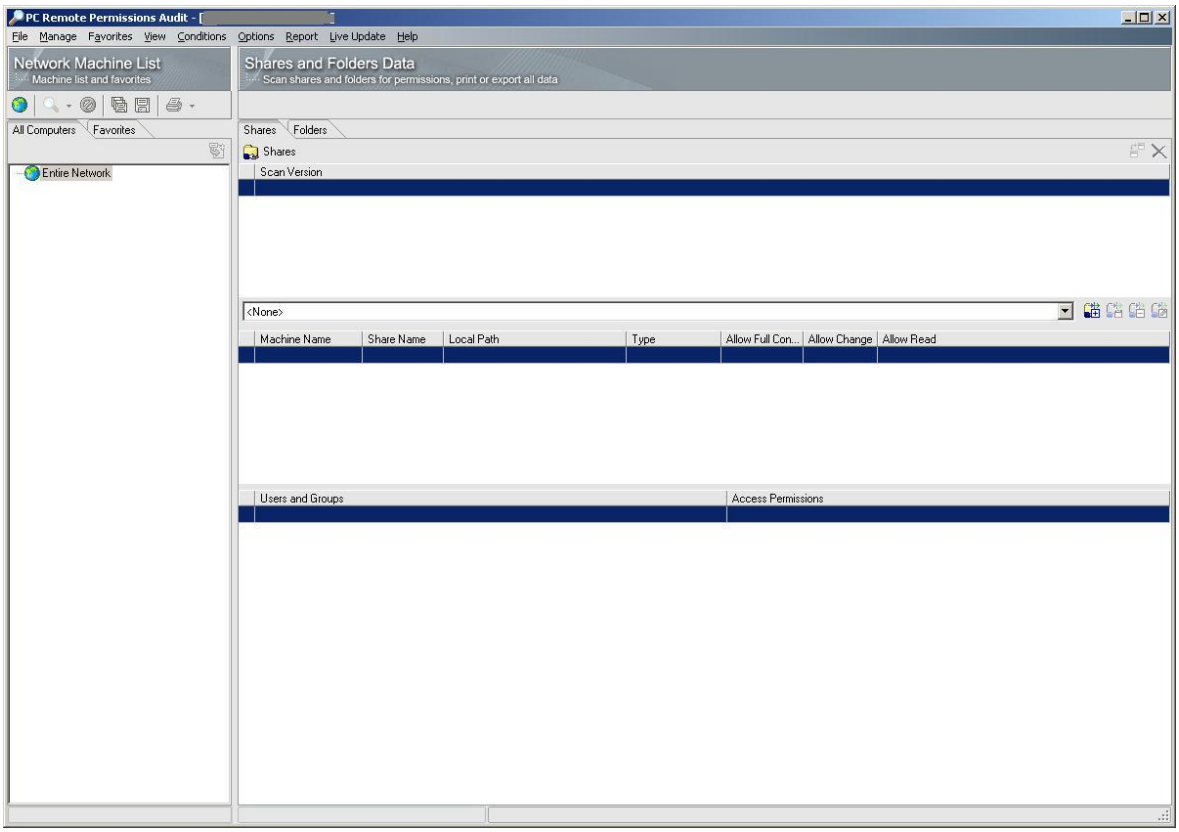

**Kuva 5. Näkymä paikallisen koneen tiedostojen ja kansioiden käyttäjäoikeuksista.**

Hyena on suunniteltu toimialueen pääkäyttäjän avuksi hallitsemaan toimialuetta (kuva 6). Ohjelma vaikutti todella monipuoliselta ja lupaavalta, joten tutustuminen siihen aloitettiin. Pian kävi kuitenkin ilmi, että kyseinen ohjelma oli todella laaja ja opetteluun kuluisi todella paljon aikaa. Monessa muodossa ohjelma vastasi muita toimialueen hallintaan tarkoitettuja ohjelmia (esim. DameWare). Ohjelma näytti sopivan päivittäiseen toimialueen hallintaan, mutta projektin tarvitseman tiedon löytäminen ja hallitseminen tuottivat vaikeuksia. Ohjelma tarjosi paljon tietoa toimialueesta, joten opinnäytetyön kannalta mielekkään tiedon oletettiin löytyvän ohjelman avulla. Hyenan mukana tuli siihen liitettynä ja erikseen ajettava ohjelma Exporter Pro. Ohjelman käyttöä ei projektin aikana ehditty testaamaan. Ennen kuin Hyenaan tutustuttiin syvällisemmin, päätettiin testata kolmas ladatuista ohjelmista.



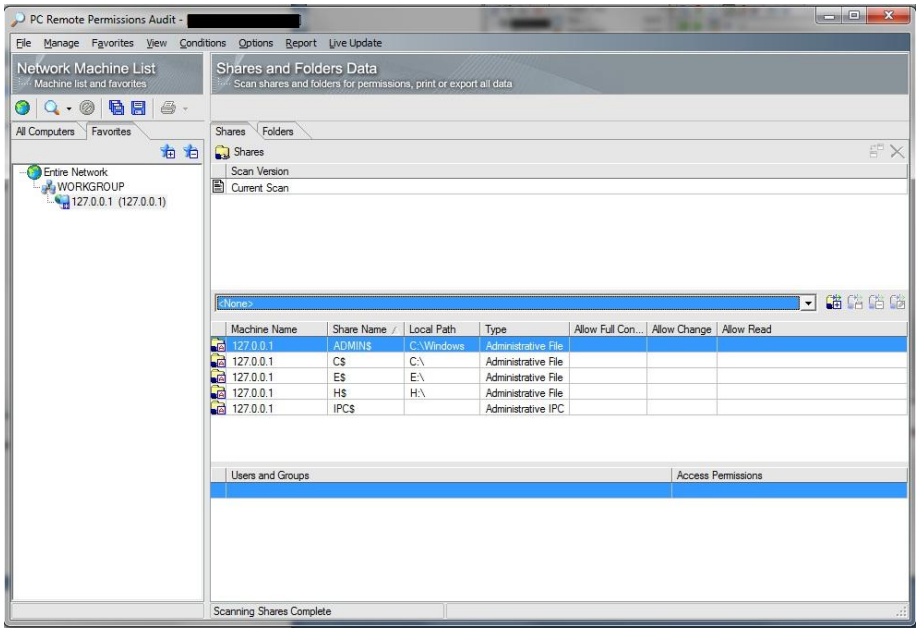

**Kuva 6. Esimerkki Hyenan pääikkunasta ja polku mukana tulevaan Exporter Pro-ohjelmaan.**

Kolmas ladatuista ohjelmista oli PC Remote Tools Oy:n valmistama PC Remote Permissions Audit ohjelma (kuva 7).




**Kuva 7. PCRPA:n pääikkuna asennuksen jälkeen.**

Ohjelma osoittautui helppokäyttöiseksi ja projektin kannalta hyvin lupaavaksi. Ensimmäiset testauskartoitukset paikalliseen työasemaan eivät kuitenkaan onnistuneet. Ongelman ratkaisuksi osoittautui muutaman ohjelman kannalta kriittisen palvelun kytkeminen päälle. Ohjelman vaatimat palvelut päätettiin asettaa automaattisesti käynnistyväksi Windows:in käynnistyessä. Palvelujen käynnistämisen jälkeen testauskartoitus onnistui paikalliselle koneelle. Onnistunut kartoitus testikoneesta voidaan nähdä kuvasta 8. Työasemasta saatiin kerättyä järkevän näköistä tietoa, joten ohjelma päätettiin ottaa kunnolliseen testiin. Kohteena oli viereinen työasema. Näin selvitettiin onnistuuko verkon yli tehtävät kartoitukset. Ennen työaseman kartoitusta varmistettiin, että kohdekoneelta oli käynnistettynä ohjelman vaatimat palvelut. Verkon yli tapahtunut kartoitus onnistui ja työasemasta saatiin hyvin samankaltaista tietoa, kuin testikoneesta (kuva 8). Testikartoituksia tehtiin testikoneelle ja käytössä olleelle työasemalle vielä useita kertoja. Ohjelmaan tutustuttiin tarkemmin ja ohjelman tarjoamaa tiedonsuodatusta kokeiltiin menestyksellisesti. Päätettiin, että ohjelmalla tehdään muutama testikartoitus projektiin määritetyille testipalvelimille, jotta nähtiin voidaanko kaikki kartoitukset suorittaa sillä. Alustavat kartoitukset testipalvelimille onnistuivat hyvin, joten ohjelman käyttöä päätettiin jatkaa eikä muihin ohjelmiin käytetty tässä vaiheessa enempää aikaa.

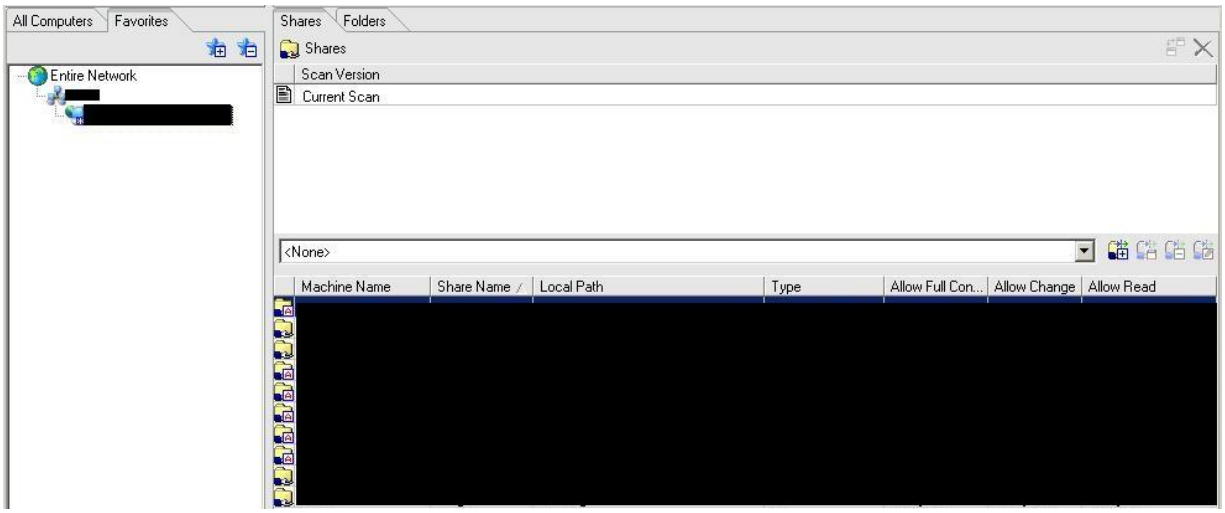



**Kuva 8. Testikoneesta tehty kartoitus.**

### 4.3.6 Kartoitukset PC Remote Permission Audit -ohjelmalla

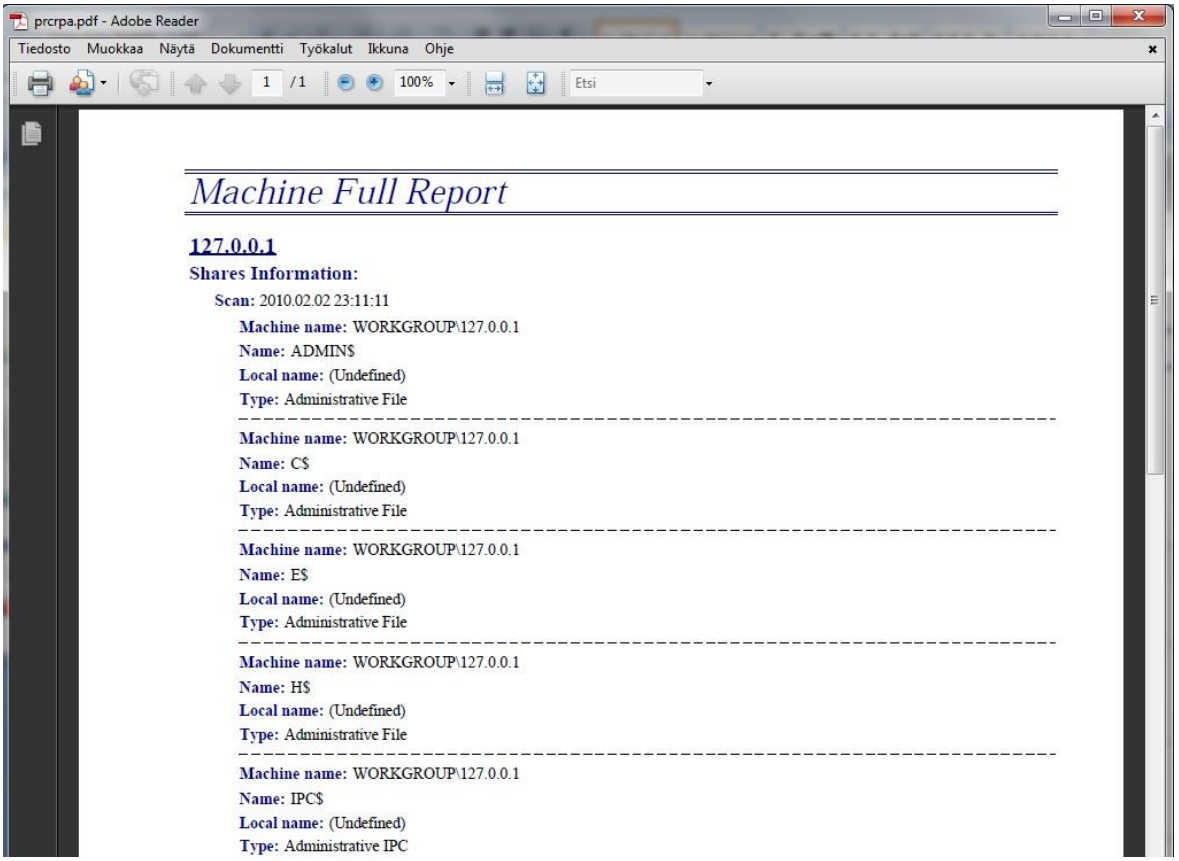
Testipalvelimille ajettiin muutamat alustavat kartoitukset, jotta ohjelman toiminta varmistettaisiin (kuva 9). Palvelimille otettiin etäyhteys, jotta tiedostojakojen ja paikallisten tiedostojen tietoja voitiin verrata ohjelman antamiin tietoihin. Ohjelma todettiin toimivaksi. Testikartoituksien aikana ilmeni kuitenkin yksi ohjelman rajoituksista. Rajoituksen syynä oli tuotantoverkon koko.

Kartoituksien seuraava vaihe oli tiedon suodatus. Kuten Nessusksella tehdyissä kartoituksissa myös tämän ohjelman avulla saatua tietoa jouduttiin suodattamaan, jotta haluttujen käyttäjäryhmien oikeudet voitaisiin paremmin kartoittaa. Suodattimia tehtäessä ohjelman hankaluudet käsitellä tuotantoverkon kokoa ilmenivät jälleen. Käyttäjäryhmiä etsittäessä ohjelma hidastui huomattavasti ja kaatuili. Ongelmat pystyttiin kuitenkin kiertämään syöttämällä kohdekoneiden ja käyttäjäryhmän tiedot manuaalisesti. Opinnäytetyön kannalta tietojen manuaalisen syöttämisen mahdollisuus osoittautui tärkeäksi, sillä ilman sitä ohjelmaa ei olisi voitu käyttää lopullisissa kartoituksissa. Toimialueelta toiselle tapahtunut kartoitus ei toiminut halutulla tavalla. Ongelma kierrettiin asentamalla ohjelma etäyhteyden avulla kohdepalvelimelle ja tekemällä kartoitus sitä kautta. Pysyvämpää ratkaisua ongelmaan ei opinnäytetyön aikana keksitty.




**Kuva 9. Testikartoitukset kohdepalvelimelle onnistuivat.**

Kartoituksien jälkeen ohjelman avulla luotiin yhteenveto kerätystä tiedosta. Yhteenvedot oli mahdollista luoda käyttämään Microsoft Excel -tai PDF-formaattia (kuva 10 ja taulukko 1). Kuhunkin yhteenvetoon otettiin mukaan vain projektin kannalta olennaiset tiedot. Ilman tiedon suodatusta pdf-tiedostoista tuli kymmenien sivujen pituisia eivätkä ne palvelleet projektin tavoitteita. Jokaisesta testipalvelimesta tehtiin yhteenveto. Yhteenvetojen tiedot liitettiin tietoturvaraportteihin ja tulokset analysoitiin.




**Kuva 10. Esimerkki PCRPA:n luomasta pdf-raportista.**

**Taulukko 1. Esimerkki PCRPA:n luomasta excel-raportista.**

# *Machine Shares Report*

**127.0.0.1**

**Shares Information:**

| | |
|---|---|
| **Scan:** | |
| **Machine nan** | WORKGROUP\127.0.0.1 |
| **Name:** | ADMIN$ |
| **Local name:** | |
| **Type:** | Administrative file |
| **Machine nan** | WORKGROUP\127.0.0.1 |
| **Name:** | C$ |
| **Local name:** | |
| **Type:** | Administrative file |
| **Machine nan** | WORKGROUP\127.0.0.1 |
| **Name:** | E$ |
| **Local name:** | |
| **Type:** | Administrative file |
| **Machine nan** | WORKGROUP\127.0.0.1 |
| **Name:** | H$ |
| **Local name:** | |
| **Type:** | Administrative file |
| **Machine nan** | WORKGROUP\127.0.0.1 |
| **Name:** | IPC$ |
| **Local name:** | |

## 4.4 Tuloksien raportointi ja ohjelmien käyttöoppaan laatiminen

Opinnäytetyön viimeisenä vaiheena oli tietoturvakartoituksissa saatujen tuloksien raportointi ja analysointi. Raportoinnin ohella laadittiin raporttipohja, jonka avulla tulevien kartoituksien raportointi helpottuisi. Lisäksi käytetyistä ohjelmista laadittiin pikaoppaat.

### 4.4.1 Raportointipohja ja raportointi

Raportointivaihe oli projektin aikaa vievin osuus. Kaikkiaan raporttien ja raportointipohjan kirjoittamiseen käytettiin aikaa noin kolmannes koko projektin ajasta. Kustakin testipalvelimesta ja ISA-julkaisupalvelimesta kirjoitettiin Microsoft Word 2003 -tekstinkäsittelyohjelmalla tietoturvaraportti, jossa kävi ilmi kohdepalvelimen tietoturvantaso. Lisäksi raportissa analysoitiin mahdollisten tietoturvariskien vaikutusta tuotantoverkkoon sekä mietittiin toimenpiteitä tietoturvariskien korjaamiseksi. Opinnäytetyön yhtenä tavoitteena oli luoda raportointipohja näille tietoturvaraporteille, jotta tuotantopalvelimista ja testaamatta jääneistä testipalvelimista saataisiin helposti tehtyä tietoturvaraportit. Raporttipohjan tarkoitus oli saada raporteista yhdenmukaisia ja helppolukui-

sia. Samaa pohjaa käyttämällä raporttien tekeminen nopeutuisi. Opinnäytetyön luonteen vuoksi raporttipohjaa ei voitu liittää tämän opinnäytetyön liitteeksi.

Raporttipohjan tekeminen aloitettiin miettimällä, millainen raportin runko tulisi olla, jotta se palvelisi tulevia tietoturvakartoituksia parhaiten. Tavoitteena oli luoda mahdollisimman yksinkertainen pohja, johon tulisi selkeä otsikointi ja jaottelu siitä, millaista tietoa mihinkin raportin osa-alueeseen olisi tarkoitus kirjoittaa. Raporttipohjasta ei projektin tässä vaiheessa muodostettu ns. virallista ja lomakemaista, vaan yksinomaan tietotekniikkayksikön käyttöön tarkoitettu, varsin vapaamuotoinen pohja. Raporttipohjaan tehtiin valmiiksi kansilehti, sisällysluettelo ja valmiit otsikot kommentteineen. Pohja jaettiin kohdepalvelimen esittelyyn, Nessuksella kerättyjen tietojen esittelyyn ja analysointiin, PCRPA:lla kerättyjen tietojen esittelyyn ja analysointiin ja yhteenvetoon palvelimen tietoturvasta, jossa tietojen kertaamisen lisäksi annettiin kehitysehdotukset palvelimen tietoturvaan liittyen. Kunkin otsikon alle kommentoitiin lyhyesti, minkä tyyppistä tietoa raporttiin haluttiin (esimerkiksi kohdepalvelimen esittelyosioon haluttiin palvelimen ip-osoite, nimi, laitteisto jne). Raporttipohjan hyväksyi Marko Ruotsala ja sitä käytettiin jokaisen opinnäytetyön aikana tehdyn tietoturvaraportin pohjana, jolloin sitä pystyttiin raporttien tekemisen ohella kehittämään.

Raporttipohjan avulla tehtiin jokaisesta opinnäytetyön kohteeksi määritellystä palvelimesta tietoturvaraportti. Raporttien sisältö koottiin edellisessä kappaleessa esitellyn raporttipohjan runkoa hyväksikäyttäen. Raportteja kirjoitettaessa huomattiin, että Nessuksen löytämien tietojen suodattamisesta huolimatta tietoa oli paljon. Jokaisen mahdollisen riskin yksityiskohtaista läpikäyntiä (ote Nessuksen raportista, kommentointi ja lopulta analysointi) ei koettu projektin kannalta mielekkääksi, vaan sisältöä pyrittiin tiivistämään löytöjen samankaltaisuuksien avulla. Esimerkiksi, jos kahden eri ohjelman vanhasta versiosta tuli varoitus, toinen löydöistä esiteltiin yksityiskohtaisesti ja toinen ohjelma mainittiin samassa yhteydessä. Näin raporteista saatiin helppolukuisia ilman, että tärkeää tietoa jäi käymättä läpi. Tietojen analysoinnissa pyrittiin jämäkkyyteen ja selkeyteen. Raporttien käyttäjinä oli asiantuntijoita, joten kaikkien uhkien täydellinen selitys ei ollut tarpeen. Raporteissa kerrottiin, mistä löydöt johtuivat, miksi ne oli kohdepalvelimen kannalta haitallisia ja mitä löytöjen suhteen voitaisiin tehdä. Marko Ruotsalan pyynnöstä jokaiseen raporttiin lisättiin osuus, jossa käytiin läpi ohjelmien käyttö tietoturvakartoituksen aikana. Raportteihin lisättiin lista käytettyjen ohjelmien tarvitse-

mista resursseista, kuten Windowsin palveluista tai käyttäjäoikeuksista. Raporttien valmistuttua päädyttiin myös kirjoittamaan pikaoppaat ohjelmien käyttämisestä.

### 4.4.2 Pika-asennusoppaiden laadinta

Pika-asennusoppaan laatimiseen päädyttiin, koska suppean käyttöoppaan kirjoittaminen jokaiseen kirjoitettuun tietoturvaraporttiin koettiin työlääksi ja aikaa vieväksi. Pienen ja vapaamuotoisen oppaan avulla raporttien pituus pysyi paremmin kurissa ja niiden sisältö vastasi tarkoitusta paremmin. Pikaoppaita kirjoitettiin kaksi kappaletta, yksi kummastakin lopullisissa kartoituksissa käytetyistä ohjelmista. Nessuksesta kirjoitettu opas kirjoitettiin uusimmasta 4.2 -versiosta eikä opinnäytetyön aikana käytetystä 4.0.2 -versiosta. Tulevissa kartoituksissa työvälineenä olisi hyvin todennäköisesti Nessuksen uudempi versio. Pikaoppaat tulisivat tietotekniikkatuen käyttöön, joten ne tehtiin varsin vapaamuotoisiksi. Vapaamuotoisuus oli perusteltua käyttäjien asiantuntijuuden ja ajan niukkuuden vuoksi. Oppaiden sisältö mukaili ohjelmien englanninkielisiä ohjekirjoja. Oppaisiin liitettiin kuvankaappauksia asennuksien kriittisimmistä vaiheista ja ohjeet kartoituksen suorittamisesta oletusasetuksilla. Käyttäjäryhmien kartoitukseen käytettyyn PCRPA:n oppaaseen lisättiin varoitukset ohjelman kaatumisalttiudesta ja ohjeet niiden välttämiseksi.

# 5 PROJEKTIN TULOKSET

## 5.1 Tavoitteiden täyttyminen ja tulokset

Tämän opinnäytetyön käsittelemä projekti on yhä käynnissä. Opinnäytetyö kattoi vain tämän projektin aloituksen. Opinnäytetyön alussa määritetyt tavoitteet saavutettiin suurimmalta osalta. Jokaisesta projektin alussa nimetystä testipalvelimesta ja ISA-julkaisupalvelimesta saatiin kerättyä tarpeeksi tietoa, jotta tietoturvaraportin laatiminen oli mahdollista. Testipalvelimista saatu tieto arvioitiin järkeväksi ja paikkansa pitäväksi, joten projektin aikana käytetyt kartoitusmenetelmät palvelevat projektin tarpeita myös tulevaisuudessa joko nykyisessä muodossaan tai perustana uudelle pohjalle. Opinnäytetyön aikana koituneet kustannukset ovat mitattavissa työtunneissa. Muita kustannuksia opinnäytetyö ei aiheuttanut.

Käyttäjäryhmien kartoituksessa onnistuttiin tyydyttävästi. Jokaisesta testipalvelimesta saatiin kerättyä tietoa käyttäjäryhmien oikeuksista, vaikka kartoitukseen käytetty ohjelma asettikin projektille haasteita. Käytetty ohjelma joudutaan mahdollisesti vaihtamaan. Tämä riippuu projektia jatkavista henkilöistä.

Projektin tarpeisiin laadittiin raportointipohja ja pikaoppaat. Raporttipohja toimii nykyisellään tyydyttävästi ja tarpeen mukaan se on hyvä perusta virallisemman tietoturvapohjan laadintaan. Käyttöoppaat ovat yksinkertaiset mutta riittävät tietotekniikkatuen käyttöön.

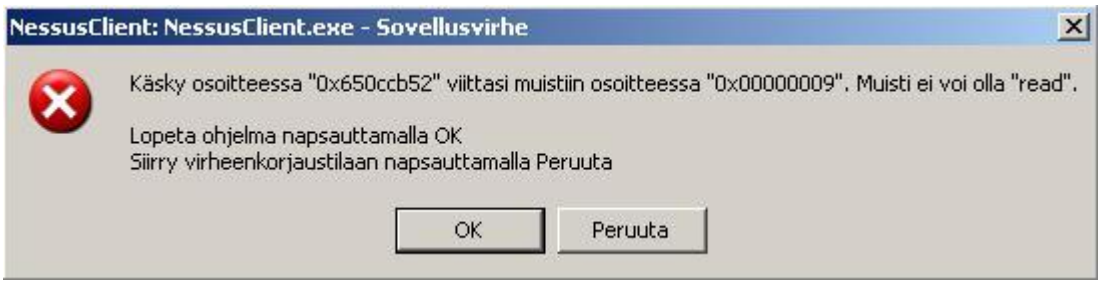
## 5.2 Projektin ongelmat

Projektin aikana kohdattiin useita eri ongelmia, joista muutamat olivat projektin toteutuksen kannalta hyvinkin merkittäviä. Tässä kappaleessa käydään läpi ongelmia, joista koitui merkittäviä haittoja projektin toteutuksen aikana. Luonteeltaan ongelmat olivat suurelta osin teknisiä ja ne ilmenivät lähinnä ongelmina käytettyjen ohjelmien kanssa. Lisäksi projektin aikana käynnissä ollut Tekplus:an ja Kuopion kaupungin atk-keskuksen yhdistyminen Istekki Oy:ksi söi hieman resursseja projektin ohjauksesta. Yhtenä

ongelmana voidaan pitää opinnäytetyöntekijän kokemattomuutta tietojärjestelmien kanssa työskennellessä. Kaikkien projektin aikana ilmenneiden ongelmien kustannukset voidaan ilmaista suoraan menetetyissä työtunneissa. Muita konkreettisia kustannuksia ongelmilla ei ollut.

Nessuksen kanssa ilmeni epäsäännöllisiä kaatumisongelmia koko projektin ajan (kuva 11). Ongelma esiintyi hyvin epäsäännöllisesti ja siihen törmättiin projektin aikana noin 10 kertaa. Nessus käynnistettiin jokaisena työpäivänä, joten kovin yleisestä viasta ei ole kyse. Kaatumista esiintyi ainoastaan testityöasemalle eikä esimerkiksi projektin käyttöön varatussa kannettavassa. Kaatuminen ilmeni jokaisella kerralla samassa vaiheessa. Kun Nessuksella oli suoritettu tietoturvakartoitus kohdepalvelimelle ja kartoituksen tuloksia haluttiin tarkastella. Käytännössä tämä tarkoitti sitä, että tehty tietoturvakartoitus jouduttiin tekemään uudestaan. Ongelman syytä ei saatu selvitettyä, mutta sen arveltiin olevan korjattavissa ohjelman uudelleen asennuksessa. Tähän ei kuitenkaan ryhdytty, sillä ongelman aiheuttamat haitat koettiin pienemmiksi kuin ohjelman uudelleenasennuksesta koituvat viivästykset.

Toinen Nessuksen käytössä ilmennyt ongelma liittyi ohjelman käyttämien ohjelmapalasien päivitykseen. Kyseessä oli ohjelman käyttämän nessus-fetch.rc tiedoston rikkoutuminen. Ohjelma antoi virheilmoituksen, jossa epäiltiin tiedoston olevan peräisin toisesta Nessus-asennuksesta. Ongelma johtui luultavasti siitä, että projektin aikana Nessus jouduttiin asentamaan testityöasemalle kahdesti lyhyen ajan välille. Ongelma ei ollut projektin kannalta kovin merkittävä, sillä ohjelman käyttämien ohjelmapalasien päivitys tehtiin Nessusta asennettaessa. Ongelma olisi todennäköisesti hävinnyt uudelleenasennuksella.

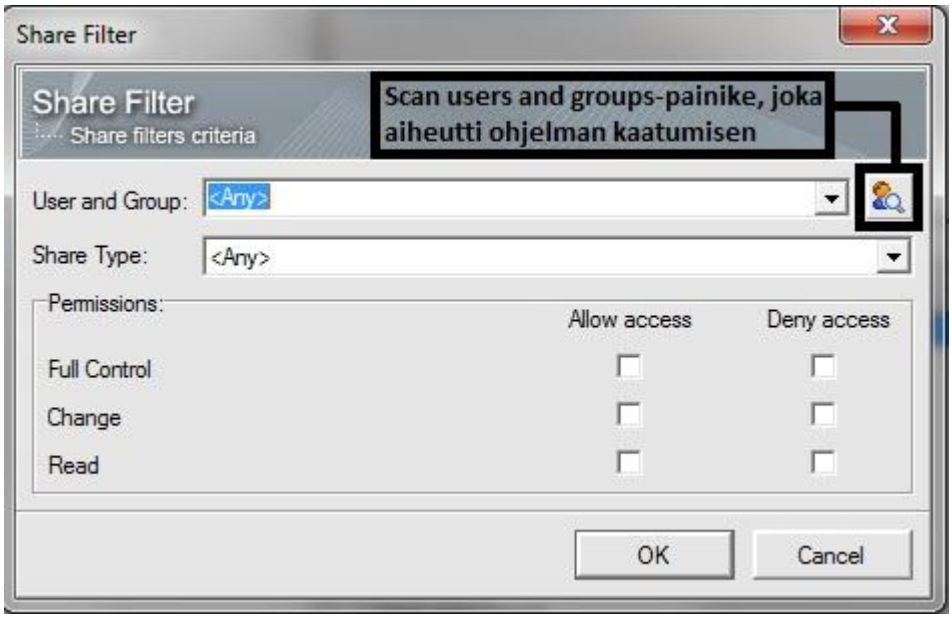



**Kuva 11. Nessus 4.0.2 antama virheilmoitus kaatumisen yhteydessä.**

Käyttäjäryhmien oikeuksien kartoitukseen käytetty PC Remote Permissions Audit aiheutti Nessusta enemmän päänvaivaa projektin aikana. PSSHP:n tuotantoverkon koko asetti ohjelmalle suuria haasteita koko projektin ajan. Ohjelman pääikkunasta käynnistettävä verkonkartoitus (kuva 7) vei ohjelmalta kymmeniä minuutteja silloin, kun se ei kaatunut toimenpiteeseen. Ongelmien syyksi arveltiin tuotantoverkon kokoa. Lisäksi ohjelma haki ainoastaan saman toimialueen koneet kun mille ohjelma itse oli asennettu. Tämä teki toimialueelta toiselle tarkastelun työlääksi ja aikaa vieväksi.

Projektin edetessä ilmeni, että toisella toimialueella sijaitsevan kohteen kartoitus ei onnistunut ilman ohjelman paikallista asennusta. Ongelma oli kierrettävissä syöttämällä tarkasteltavien koneiden tiedot manuaalisesti. Tämä ei kuitenkaan ole mielekästä, jos tarkasteltavia koneita on opinnäytetyössä käsiteltävien kuuden sijasta useita satoja. Ohjelman kaatumiset aiheuttivat osaltaan myös sen, että ohjelman rajallinen käynnistysmäärä kului hyvin nopeasti. Ohjelma tarjosi mahdollisuuden tehdä vaihtoehtoisia käyttäjätilejä, mutta ilmeisesti isäntäkoneen ja toisen toimialueen kohdekoneen tuli jakaa käyttäjätilitiedot. Tätä ongelmaa ei saatu opinnäytetyön aikana ratkaistua. Ohjelman ohjekirja ei tarjonnut ongelmaan kovinkaan paljoa apua, joten on myös mahdollista, että kyseessä oli väärästä syntaksista johtuva ongelma. Projektin kannalta oli onni, että ohjelma oli hyvin nopea asentaa ja poistaa. Sen vuoksi ohjelma pystyttiin asentamaan paikallisesti kohdekoneelle hyvin nopeasti. Yllä mainittujen syiden vuoksi oli selvää, että ohjelman korvaajaksi olisi syytä löytää toinen ohjelma tai keino. Opinnäytetyön puitteissa tämä ei kuitenkaan onnistunut työhön käytettävän ajan rajallisuuden vuoksi.

Tuotantoverkon kokoon liittyneet rajoitukset ohjelmassa ilmenivät myös käyttäjäryhmien automaattisessa kartoituksessa. Ohjelmalla on mahdollista listata käyttäjäryhmät suodatinta tehtäessä (kuva 12). Painettaessa kuvassa 12 nähtävää painiketta ohjelma kaatui. Syyn arveltiin olevan PSSHP:n tuotantoverkon koko ja eri käyttäjien ja käyttäjäryhmien määrä. Ongelma pystyttiin kiertämään syöttämällä käyttäjäryhmä käsin. Syntaksi tähän oli yksinkertainen ja looginen eikä tämä ongelma haitannut projektin etenemistä.




**Kuva 12. PCRPA:n ongelma suodatinta tehtäessä.**

Yhtenä ongelmana projektin kannalta voidaan pitää sitä, ettei ohjelmien testaukseen ja eri asetusten säätöön voitu käyttää enempää aikaa. Tuotantoverkko asetti projektille haasteita, sillä verkon toimintaa ei ollut lupa häiritä.

Opinnäytetyön tekijän kokemattomuutta tietojärjestelmistä voidaan pitää ongelmana. Vaikka tietoturva oli aiheena tuttu, oli tiedon soveltaminen laajaan tietojärjestelmään välillä haastavaa. Työaikaa kului paljon siihen, että opinnäytetyön tekijä joutui ottamaan selvää, miten yksinkertaisimpiakin toimenpiteitä saatiin tehtyä turvallisesti. Kokemattomuus heijastui osaltaan ohjelmien käyttöön ja opinnäytetyön onnistumiseen.

Tekplus:an ja Kuopion atk-keskuksen yhdistyminen aiheutti projektille resurssiongelmia, sillä se työllisti projektia johtanutta Marko Ruotsalaa ja koko Tekplus:aa hyvin paljon, joten projektin kannalta tärkeiden asioiden käsittelyä jouduttiin välillä lykkäämään.

## 5.3 Kehitysehdotukset

Projektin jatkon kannalta olisi tärkeää, että käytettyihin ohjelmiin tutustuttaisiin paremmin. Projektin aikana Nessusta käytettiin oletusasetuksilla. Ohjelma on kuitenkin äärettömän monipuolinen eikä sitä käytetty projektin aikana niin hyvin kuin olisi mah-

dollista. Tulevia kartoituksia varten voisi olla järkevää, että ohjelman lisäasetuksia ja esim. tietokantoja koskevia asetuksia testataan. Asetuksia muuttamalla kohteista saataisiin luultavasti parempaa ja yksityiskohtaisempaa tietoa.

Käyttäjäoikeuksien kartoituksia varten suosittelisin miettimään, olisiko olemassa parempaa vaihtoehtoa kuin PC Remote Permissions Audit. Opinnäytetyön aikana käytetty ohjelma on PSSHP:n kokoiseen verkkoon liian kevyt ohjelma, mikä aiheutti kartoituksien aikana hankaluuksia. Ohjelmalla pystyy tekemään tarvittavat kartoitukset mutta se ei ole kovin helppokäyttöinen toisten toimialueiden puolella olevien palvelimien kartoituksiin.

Raportointia varten tehty raporttipohja on nykyisellään toimiva. Se on tosin hyvin epävirallinen ja tietotekniikkatuen käyttöön rajattu. Ulkopuolisia raporttipohja ei palvele. Raporttipohjasta voitaisiin tehdä virallisempi ja kaavakemaisempi, jolloin se olisi helpompi täyttää.

# LÄHTEET


1. Microsoft. Windows-palvelimien historia. Päivitetty 30. kesäkuuta 2003. [verkkodokumentti] viitattu 20.3.2010. http://www.microsoft.com/windows/WinHistoryServer.mspx

2. Ruotsala, Marko. (2005) Ohjelmistojen ja tietoturvapäivitysten jakelu Pohjois-Savon sairaanhoitopiirin työasemaympäristössä. Tietotekniikan koulutusohjelma. Savonia amk, tekniikka, Kuopio.

3. Microsoft. Windows Server 2008 R2 yleiskuva. [verkkodokumentti] viitattu 20.3.2010. http://www.microsoft.com/windowsserver2008/en/us/overview.aspx

4. Microsoft. ISA-palvelimen yleiskuva. [verkkodokumentti] viitattu 20.3.2010. http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/overview.aspx

5. Microsoft. ISA-palvelimen ominaisuudet. [verkkodokumentti] viitattu 20.3.2010 http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/features.aspx.

6. Elizabeth D Zwicky, Simon Cooper & D. Brent Chapman. Suomentanut Pekka Saxberg - *Internet-Palomuurien rakentaminen*. Talentum media 2001.

7. Ruohonen, Mika. (2002). *Tietoturva*. Docendo Finland

8. Kirves, Antti, *Mitä on spyware?* Digitoday 26.3.2003. [verkkodokumentti] viitattu 20.3.2010. http://www.digitoday.fi/tietoturva/2003/03/26/mita-on-spyware/200310595/66

9. Järvinen, Petteri. 2010. Varo Scarewarea. *Tietokone*, 1/2010.

10. CISCO CCNP2 version 5.0 (2007). [verkkodokumentti] viitattu 15.3.2010. Kurssimateriaaliin rajoitettu pääsy (Savonia-Amk opiskelijat ja henkilökunta). http://netacad.savonia-amk.fi/CCNP/CCNP2_v50_en/ch5/main.html.